Capítulo 5

Governança da Cibersegurança e Privacidade dos Dados sob a Perspectiva das Cidades Inteligentes

Radames Giona, Fernando Nakayama, Edson T. de Camargo, Michele Nogueira

Resumo

Este capítulo aborda a governança em cibersegurança e privacidade dos dados sob a ótica das cidades inteligentes, explorando os desafios, conceitos fundamentais e frameworks regulatórios mais relevantes para a proteção de infraestruturas urbanas digitais. A partir da análise de modelos como o NIST CSF, ISO/IEC 27001 e COBIT 2019, o texto discute como adaptar esses frameworks ao ecossistema urbano altamente conectado e dependente de tecnologias IoT. Além disso, realiza uma revisão sistemática da literatura para identificar lacunas, tendências tecnológicas e boas práticas voltadas à governança da segurança de dispositivos conectados. Ao integrar fundamentos teóricos, diretrizes práticas e evidências empíricas, o capítulo oferece uma contribuição relevante para a construção de cidades inteligentes mais seguras, resilientes e voltadas à proteção dos direitos digitais dos cidadãos.

Abstract

This chapter addresses cybersecurity and data privacy governance from the perspective of smart cities, exploring key challenges, foundational concepts, and the most relevant regulatory frameworks for protecting urban digital infrastructures. Through the analysis of models such as NIST CSF, ISO/IEC 27001, and COBIT 2019, it discusses how these frameworks can be adapted to the highly connected urban ecosystem driven by IoT technologies. In addition, it presents a systematic literature review to identify research gaps, emerging technologies, and best practices for governing the security of connected devices. By integrating theoretical foundations, practical guidelines, and empirical evidence, the chapter offers a valuable contribution to the development of safer, more resilient, and privacy-aware smart cities.

5.1. Introdução

A adoção de iniciativas de cidades inteligentes impulsionou a digitalização dos serviços urbanos, tornando-os mais eficientes e conectados. Entretanto, essa transformação amplia significativamente a vulnerabilidade e ameaças cibernéticas, especialmente devido ao aumento e gerenciamento de grandes volumes de dados sensíveis e informações de infraestruturas [Ahmadi-Assalemi et al. 2020, Frandell and Feeney 2022]. Embora mecanismos de segurança, como *firewalls*, criptografia e ferramentas antimalware, sejam fundamentais para a proteção das infraestruturas digitais, a ausência ou inadequação de políticas de cibersegurança representa um desafio crítico, dificultando a implementação de práticas eficazes de proteção [Sarker et al. 2021, Hatcher et al. 2020].

No ambiente urbano, as soluções baseadas em Internet das Coisas (IoT, do inglês *Internet of Things*) e no próprio dispositivo móvel do cidadão se tornam cada vez mais comuns. Os dados coletados são primordiais para fornecer "inteligência" às soluções desenvolvidas. Esses dados alimentam aplicativos da cidade, ajudam na gestão da cidade, orientam a execução de políticas públicas, bem como fornecem ferramentas para controle social por meio de portais de dados abertos [Goumopoulos 2024]. Exemplos de dados da cidade são: fluxo de tráfego, dados ambientais (por exemplo, qualidade do ar/água), níveis de ruído, áreas verdes, consumo/geração/perdas de energia, volume/tipo de resíduos, equipamento urbano, estado da infraestrutura urbana e outros.

Compreender a governança em cibersegurança e seus efeitos é fundamental, pois ela permite a formulação de políticas e estratégias integradas, assegurando a proteção de dados, a continuidade operacional e o desenvolvimento sustentável de cidades inteligentes. Destaca-se que é crucial para as cidades inteligentes contar com uma governança eficiente em segurança cibernética para garantir a proteção dos sistemas e dos serviços urbanos. Entende-se por governança, nesse contexto, como uma estrutura conceitual revisável para investigações empíricas da realidade e como um projeto político para alcançar objetivos específicos ou ainda não realizados a serem decididos democraticamente [Wilkins and Mifsud 2024]. Essa gestão, *i.e.*, o conjunto de práticas e diretrizes que orientam a governança em segurança cibernética, é estabelecido via diretrizes e métodos que garantam a integridade e a segurança dos dados, redes e sistemas e promovam o desenvolvimento tecnológico e a interoperabilidade, incentivando novas ideias [Serrano et al. 2022].

A ausência de regulamentações específicas representa um grande desafio para o desenvolvimento de cidades inteligentes seguras, pois, sem diretrizes claras, aumenta-se o risco de vulnerabilidades cibernéticas e o comprometimento de dados sensíveis. A falta de políticas apropriadas compromete a confiança pública e a eficácia das cidades inteligentes [Elmaghraby and Losavio 2014]. A maioria dos dispositivos integrantes das cidades inteligentes é projetada com foco em funcionalidade e custo, mas frequentemente negligencia aspectos essenciais de cibersegurança, tornando-os vulneráveis a ataques cibernéticos. Essa fragilidade impacta diretamente sistemas críticos, como as redes de energia e transporte, comprometendo a infraestrutura urbana [Meneghello et al. 2019]. Ao mesmo tempo que as tecnologias IoT e móveis avançam rapidamente, é necessário manter atualizadas as políticas de segurança cibernética para garantir a governança adequada no ambiente digital. Os governos e as organizações precisam encontrar um equilíbrio entre

a evolução tecnológica e a mitigação dos riscos para assegurar a resiliência e a confiança das infraestruturas urbanas [Xagoraris et al. 2023].

Entre os objetivos da governança em cibersegurança estão o fortalecimento da segurança nos ambientes digitais, a gestão de riscos e o cumprimento de regulamentações, com um enfoque claro na definição de responsabilidades e na implementação de medidas de monitoramento e resposta a incidentes. Ou seja, a governança em cibersegurança busca assegurar que as organizações mantenham um ambiente seguro e resiliente contra ameaças cibernéticas. Em ambientes urbanos, no contexto das cidades inteligentes, a governança de cibersegurança se torna ainda mais complexa devido à digitalização crescente e ao uso de tecnologias como *IoT*, *big data*, redes de comunicação (como as de longo alcance e baixa potência e as redes 5G) e a inteligência artificial.

Este capítulo oferece uma análise abrangente sobre a governança em cibersegurança e privacidade dos dados no contexto das cidades inteligentes. Na Seção 5.2, são abordados conceitos fundamentais de governança, cibersegurança e suas relações com dispositivos conectados, além dos desafios críticos de governança, como a interoperabilidade de dispositivos *IoT* e a mitigação de riscos em ambientes urbanos. A Seção 5.3 apresenta uma análise de *frameworks* de governança amplamente adotados — como o NIST CSF, a ISO/IEC 27001 e o COBIT 2019 — com foco em sua aplicabilidade às cidades inteligentes. Na Seção 5.4, é realizada uma revisão sistemática da literatura para identificar lacunas de pesquisa, aplicações concretas e tecnologias voltadas à governança da segurança de dispositivos conectados no meio urbano. A Seção 5.5 apresenta práticas relevantes com base em estudos de caso. A Seção 5.6 discute desafios específicos relacionados à proteção e à gestão de dispositivos *IoT* e móveis em ambientes urbanos e a Seção 5.7 trata de tendências emergentes no campo, oferecendo recomendações estratégicas. Ao articular fundamentos teóricos, estruturas práticas e achados empíricos, o capítulo oferece subsídios valiosos para formuladores de políticas, gestores públicos e pesquisadores que atuam na construção de cidades inteligentes mais seguras, resilientes e sensíveis à privacidade dos cidadãos.

5.2. Fundamentos

Esta seção apresenta os conceitos relacionados à governança de cibersegurança sob a perspectiva de cidades inteligentes. A seção inicia com os fundamentos relacionados à *IoT* e às cidades inteligentes, incluindo sua conceituação, aplicações e exemplos. Na sequência, detalham-se os principais conceitos de governança de cibersegurança, incluindo a motivação e os principais objetivos ao adotar a governança de cibersegurança para estruturar um ambiente digital. A seção termina descrevendo os conceitos de cibersegurança, como disponibilidade, integridade, confidencialidade, privacidade, autenticação e autorização, e ainda os fundamentos importantes acerca de vulnerabilidades, ameaças e ataques.

5.2.1. Internet das Coisas e Cidades Inteligentes

A definição de cidades inteligentes varia conforme o enfoque (tecnológico, social, ambiental). Este capítulo segue a definição de cidades inteligentes como ambientes urbanos que utilizam tecnologias digitais — ex. *IoT*, *big data*, inteligência artificial e redes de comunicação avançadas — para melhorar a qualidade de vida dos cidadãos, otimizar a

gestão de recursos e serviços públicos, promover a sustentabilidade e fomentar a participação cidadã. Essas cidades integram infraestrutura física, tecnologia da informação e processos organizacionais para oferecer soluções inovadoras em áreas como mobilidade, segurança pública, saúde, energia, educação e governança. Embora não haja uma definição universalmente aceita para o conceito de cidades inteligentes, este capítulo reforça que o objetivo principal das cidades inteligentes é aprimorar a qualidade de vida dos cidadãos, utilizando Tecnologias da Informação e Comunicação (TICs) para tornar os serviços mais eficientes, sustentáveis e integrados — promovendo, assim, um ambiente urbano mais responsivo e resiliente.

Nesse contexto de cidades inteligentes, destaca-se a tecnologia *IoT* como um paradigma de comunicação [Gracias et al. 2023, Goumopoulos 2024]. Na *IoT*, "coisas" ou objetos, outrora incapazes de se comunicar com uma pessoa ou um sistema computacional, agora estão equipados com sensores, atuadores, circuitos eletrônicos, *software* e conectividade que lhes permitem coletar e trocar dados entre si e com a Internet. Sensores, circuitos eletrônicos e *software* embarcado transformam um objeto em um objeto inteligente, permitindo que ele "veja" (monitore), "ouça" (receba dados), "pense" (processe) e execute tarefas. Caracteriza-se um objeto inteligente como um sensor avançado, dotado da capacidade de coletar informações provenientes do ambiente, tais como temperatura, umidade, localização geográfica, frequência cardíaca, bem como imagens de ambientes internos e externos [Camargo et al. 2024].

A conectividade, viabilizada predominantemente por meio de redes sem fio, permite que tais objetos estabeleçam comunicação com o meio externo – notadamente com a Internet. Essa interação possibilita o envio e o recebimento de dados e comandos, com o propósito de cumprir funções específicas e úteis. As informações transmitidas são processadas e armazenadas em serviços de computação em nuvem, o que viabiliza o controle remoto dos dispositivos inteligentes, permitindo-lhes executar ações programadas e coordenar atividades entre si. Dessa forma, a *IoT* configura-se como uma extensão da Internet convencional, fazendo uso de sua infraestrutura, de seus protocolos padronizados e de suas propriedades distribuídas.

A Figura 5.1 ilustra a arquitetura IoT em um modelo com três ou cinco camadas. No modelo de três camadas, a **camada de percepção**, também chamada de camada de sensoriamento, representa os objetos físicos e é responsável por coletar dados dos sensores e atuadores (ex. valores de temperatura, umidade, peso, movimento, vibração, localização) e repassá-los para a camada de rede. Os dispositivos *IoT* seguem uma organização básica geralmente composta por unidade de processamento, unidade de comunicação, sensores/atuadores e fonte de energia. A **camada de rede** realiza a transmissão dos dados e define o protocolo empregado na comunicação, a interface de comunicação e o roteamento. Nessa tarefa, é comum o uso de padrões e tecnologias sem fio, voltados ao baixo consumo de energia, como o padrão 802.11 (conhecido como WiFi), 5G, *Long Range* (LoRa), *Bluetooth Low Energy* (BLE), *ZigBee*, entre outras. A **camada de aplicação** faz a composição dos dados para entregar um serviço para a aplicação, com foco em protocolos que consomem pouca largura de banda, como o *Constrained Application Protocol* (CoAP), *Message Queuing Telemetry Transport* (MQTT), *Extensible Messaging and Presence Protocol* (XMPP) e *Advanced Message Queuing Protocol* (AMQP).

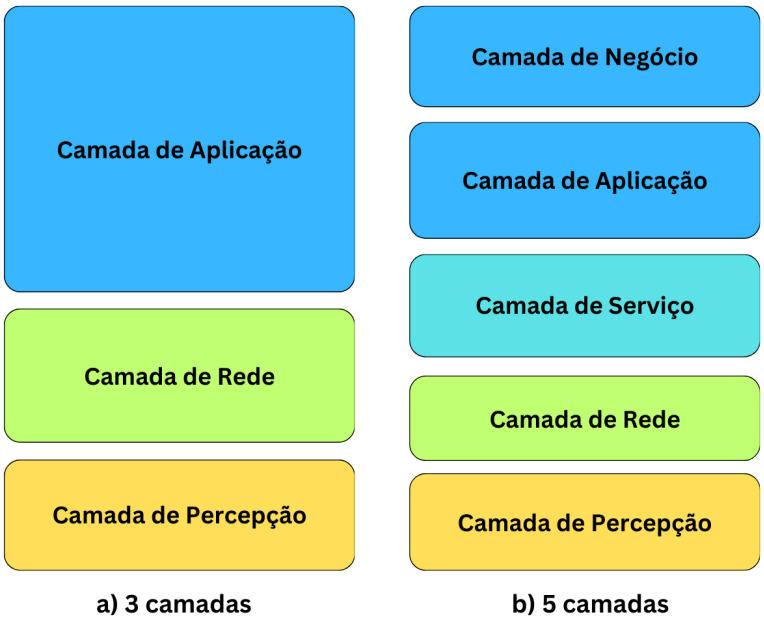

Figura 5.1: Arquiteturas de camadas para IoT (adaptado de [Pastório et al. 2020]).

No modelo de cinco camadas, a **camada de negócio** atua como a camada superior, responsável pelo controle e gerenciamento de serviços *IoT* fornecidos pela camada de Aplicação. A **camada de serviço** atua como uma camada intermediária, realizando solicitações de serviços, agregando e processando dados e implementando funcionalidades generalizadas. As demais camadas (aplicação, rede e percepção) seguem as mesmas definições do modelo em 3 camadas.

A adoção do conceito de *IoT* no contexto urbano promove a transformação das cidades em cidades inteligentes por meio da incorporação de dispositivos aptos a identificar variáveis ambientais, processar os dados captados e interpretar as condições do ambiente, reagindo de maneira adequada. Um exemplo disso é o semáforo inteligente, que recebe informações relativas ao fluxo e ao volume de veículos em determinadas vias, bem como a presença de pedestres aguardando a travessia. A partir da análise desse cenário, o dispositivo toma decisões como priorização do tráfego em ruas mais congestionadas ou a liberação da travessia quando houver pedestres efetivamente aguardando.

A Figura 5.2 ilustra a arquitetura de *IoT* em funcionamento em uma cidade inteligente. Os sensores e atuadores estão distribuídos pelo ambiente urbano, coletando dados e transmitindo-os para a Internet. Uma rede de comunicação conecta esses dispositivos entre si e à nuvem, viabilizando a troca contínua de informações. Os dados armazenados na nuvem são então processados e transformados em informações relevantes, apresentadas em painéis de controle (*dashboards*) acessíveis a gestores públicos, empresas e à população. Conforme representado na Figura 5.2, além dos dispositivos de *IoT*, outros componentes essenciais sustentam esse ecossistema, como a infraestrutura de comunicação, plataformas de *software* e ferramentas de visualização de dados — todos fundamentais para a implementação eficaz da IoT em contextos urbanos.

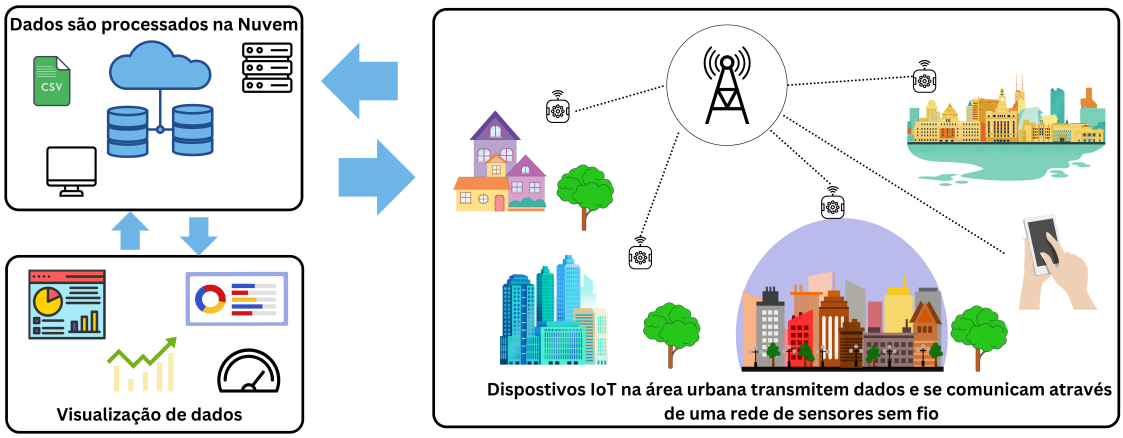

Figura 5.2: IoT em um ambiente urbano (adaptado de [Camargo et al. 2024])

Os desafios para concretizar a visão de uma cidade inteligente são diversos e incluem desde a integração e interoperabilidade entre diferentes tecnologias e atores, a tolerância a falhas, confiabilidade nas medidas obtidas dos sensores, muitas vezes sensores de baixo custo, e na transmissão dos dados [Slongo et al. 2024, Pastório et al. 2023, Lee et al. 2021, Camargo et al. 2021, Pastório et al. 2020, **?**]. Além disso, com um número estimado de mais de 1 bilhão de infraestruturas inteligentes para serviços urbanos digitais, pesquisadores e especialistas em segurança alertam para a necessidade de atenção especial à questão da cibersegurança das cidades inteligentes [Demidov et al. 2018, Pavlenko and Zegzhda 2018].

As cidades inteligentes estão expostas a ataques cibernéticos complexos a infraestruturas críticas que podem interromper sistemas automatizados e invadir a comunicação entre dispositivos inteligentes. A invasão ou infecção de um único dispositivo conectado leva a danos em cascata, resultando no risco de roubo de uma grande quantidade de dados de cidadãos e consumidores, incluindo informações pessoais identificáveis [Ometov et al. 2019]. Para alcançar esse equilíbrio, a governança da cibersegurança neste contexto é essencial, como será foco das próximas seções deste capítulo.

5.2.2. Governança

A crescente dependência da sociedade em tecnologias digitais destaca a necessidade de uma governança eficaz, garantindo que os benefícios dessas tecnologias sejam aproveitados enquanto os riscos são adequadamente gerenciados. De forma direta e simples, a governança significa encontrar um equilíbrio entre controle e conformidade a regras, políticas e leis, de um lado, e a entrega rápida de resultados e desempenho, de outro. Os interesses e objetivos desses dois lados são muitas vezes diferentes e até mesmo contraditórios e, portanto, atingir esse equilíbrio é um grande desafio. Diante dos aspectos sociais e políticos particulares de cada sociedade, esse equilíbrio tende a apresentar diferenças dependendo do país e região. Entretanto, ele é essencial para satisfazer conjuntamente as necessidades financeiras, operacionais, de segurança, e gestão de risco nas diferentes unidades de uma organização.

O conceito de governança de uma forma mais ampla compreende o estabelecimento das cadeias de responsabilidade, a definição do processo para mensurar a sua eficácia, o estabelecimento e a divulgação de políticas para guiar a organização a atingir seus objetivos, os mecanismos de controle para garantir conformidade e a comunicação para manter todas as partes informadas. Na aplicação do conceito de governança para tecnologia da informação (TI) de forma geral, a governança é instanciada para a perspectiva das pessoas, processos e informação com o objetivo de guiar a forma como esses ativos apoiam e se relacionam com as necessidades dos negócios. Por exemplo, a governança da nuvem é uma instância da governança SOA (*Service-Oriented Architecture*), ou seja, a aplicação da governança de TI em todo o contexto do ciclo de vida dos serviços, seus componentes e processos de negócios. A governança em outros contextos precisa então ser instanciada, tal como ocorreu na governança SOA, de TI e de sistemas em nuvem.

De forma geral, um modelo de governança compreende os seguintes pilares a serem definidos de forma específica: os *princípios*, os *papéis das entidades e suas responsabilidades*, as *diretrizes para as decisões*, o *método* a ser empregado, os *processos fundamentais* para a governança e a *plataforma de apoio*. Os princípios guiam os objetivos e as metas a serem perseguidas na governança, assim como as métricas a serem continuamente observadas e mensuradas com o objetivo de acompanhar e garantir que as metas sejam alcançadas. Os papéis e as responsabilidades das entidades envolvidas são definidos com o objetivo de facilitar o alinhamento das expectativas entre a parte técnica e os negócios no momento de tomada de decisão. As diretrizes para as decisões contemplam um conjunto de políticas, guias, melhores práticas e padrões definidos e alinhados com os negócios. O método estabelece a abordagem a ser aplicada no ciclo de vida do sistema, definida em consonância com o modelo geral de governança. Os processos fundamentais são aqueles relacionados às exceções, à conformidade e à comunicação. A plataforma integra as tecnologias habilitadoras utilizadas na execução da governança.

A governança de cibersegurança tem como objetivo equilibrar o cumprimento de normas, leis e regulamentos com a necessidade de eficiência e inovação no uso da tecnologia. Essa busca por equilíbrio é desafiadora, pois o fortalecimento da segurança impacta a usabilidade e a agilidade dos serviços digitais. Além disso, fatores sociais, políticos e econômicos influenciam a forma como a governança de cibersegurança é estruturada em diferentes setores e regiões. Um modelo eficaz de governança de cibersegurança é essencial para garantir a resiliência operacional, a conformidade regulatória e a proteção contra ameaças cibernéticas. Ele envolve diversos aspectos fundamentais. Os *princípios orientadores* definem diretrizes e métricas para avaliar a eficácia das políticas de segurança. Eles estabelecem parâmetros claros para a proteção dos ativos digitais e ajudam a alinhar as estratégias organizacionais com os requisitos regulatórios e operacionais. Os *papéis e responsabilidades* devem ser bem definidos para garantir o alinhamento entre gestores, profissionais de TI e *stakeholders*. A clareza nas atribuições de cada participante do processo de segurança minimiza riscos e melhora a coordenação das ações preventivas e reativas diante de ameaças cibernéticas [Nogueira 2022].

As *diretrizes para decisões* abrangem políticas, melhores práticas e padrões regulatórios que servem de base para a implementação de medidas de segurança eficazes. Esses elementos orientam a gestão de riscos e a conformidade com normativas nacionais e internacionais, como a ISO/IEC 27001 e o NIST Cybersecurity Framework. Os

métodos de gestão estabelecem abordagens para implementar e monitorar medidas de segurança. Eles incluem processos de auditoria contínua, análise de vulnerabilidades e resposta a incidentes, garantindo que as organizações possam se adaptar rapidamente às novas ameaças e desafios tecnológicos.

Os *processos fundamentais* envolvem a gestão de riscos, a conformidade e a resposta a incidentes cibernéticos. Uma abordagem estruturada para esses processos permite a antecipação de problemas e a mitigação eficiente de impactos, reduzindo o tempo de recuperação em caso de ataques. As *plataformas tecnológicas* sustentam a execução das estratégias de segurança. A adoção de soluções robustas, como sistemas de monitoramento avançado, inteligência artificial para detecção de ameaças e criptografia forte, são fundamentais para proteger dados e garantir a integridade das operações.

A governança de cibersegurança se difere da simples gestão operacional da segurança da informação. Enquanto a gestão tem um foco mais técnico e reativo, a governança exige uma abordagem estratégica, envolvendo decisores de alto nível. Ademais, a governança no tocante à cibersegurança deve atuar durante todo o ciclo de vida das soluções de segurança, desde o planejamento até a implementação e revisão periódica. Um modelo eficaz de governança de cibersegurança fortalece a transparência, otimiza recursos e melhora a proteção contra ameaças digitais. Ela é essencial para mitigar desafios técnicos e administrativos. A falta de integração entre sistemas de segurança e setores organizacionais pode gerar vulnerabilidades críticas. A redundância de controles e processos compromete a eficiência operacional e aumenta custos desnecessários. O desalinhamento entre políticas de segurança e objetivos estratégicos da organização pode resultar em brechas de segurança e ineficácia na proteção de dados. Os riscos de violação de dados e ataques cibernéticos estão em constante evolução, exigindo abordagens dinâmicas e proativas. A falta de visibilidade sobre os ativos digitais e infraestruturas críticas compromete a capacidade de resposta rápida e eficaz a incidentes.

Assim, a governança da cibersegurança compreende duas perspectivas distintas e complementares. A perspectiva interna foca no nível institucional dos ativos digitais, na eficiência dos processos e na proteção contra ameaças. Esse enfoque permite otimizar a alocação de recursos, melhorar a resiliência dos sistemas com abrangência institucional e garantir que a segurança seja parte integrante da estratégia empresarial. A perspectiva externa está voltada às normativas e políticas gerais para garantir a proteção de dados, privacidade e segurança digital. A conformidade com leis e regulamentos, como a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Geral sobre a Proteção de Dados (GDPR), é essencial para evitar penalidades e fortalecer a confiança dos usuários. Uma governança eficaz de cibersegurança assegura transparência, conformidade, segurança e inovação responsável. Dessa forma, as organizações e os governos podem utilizar a tecnologia de maneira segura, protegendo informações sensíveis e garantindo um ambiente digital confiável para todos.

A governança de cibersegurança desempenha um papel fundamental na estruturação de um ambiente digital confiável, resiliente e sustentável. As questões centrais relacionadas a esse tema pode ser organizada em quatro grandes grupos: *(i)* segurança, robustez e resiliência dos sistemas digitais; *(ii)* proteção de direitos, privacidade e regulamentação de dados; *(iii)* inovação, desenvolvimento econômico e sustentabilidade

Figura 5.3: Perspectivas da governança de cibersegurança

da segurança digital; e *(iv)* transparência, governança corporativa e responsabilidade no ecossistema digital. Esses temas refletem os desafios contemporâneos enfrentados por governos, empresas e sociedade civil na busca por políticas eficazes de cibersegurança e governança digital e são descritos em seguida.

A segurança cibernética é um dos pilares centrais da governança de cibersegurança, pois garante a integridade, disponibilidade, confiabilidade e não repúdio, entre outros conceitos relacionados aos sistemas tecnológicos. A crescente sofisticação dos ataques cibernéticos, como *ransomware*, violações de dados e ataques a infraestruturas críticas, exige um modelo de governança que priorize a resiliência e a proteção contra ameaças. Os governos e as organizações precisam adotar estruturas regulatórias que incentivem práticas como segurança por projeto (*security by design*), gestão proativa de vulnerabilidades e respostas coordenadas a incidentes cibernéticos. Além disso, a implementação de *frameworks* internacionais, como a ISO/IEC 27001 e o NIST Cybersecurity Framework, fortalece a segurança organizacional e setorial.

A governança da cibersegurança também está diretamente relacionada à proteção de direitos digitais e à privacidade dos usuários. As regulamentações como o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia e a Lei Geral de Proteção de Dados (LGPD) no Brasil estabelecem diretrizes para o tratamento responsável de informações pessoais e impõem regras sobre coleta, armazenamento e compartilhamento de dados. Além das leis, normas e padrões, a proteção da privacidade deve ser reforçada por meio de medidas técnicas e operacionais, como criptografia, anonimização de dados e controles rigorosos de acesso. Modelos de governança eficazes devem garantir que empresas e instituições adotem políticas transparentes e práticas que respeitem a soberania e os direitos dos cidadãos no ambiente digital.

A cibersegurança não pode ser vista apenas como um custo operacional, mas como um fator estratégico para a inovação e a competitividade econômica. As empresas que incorporam medidas robustas de segurança em seus produtos e serviços não apenas protegem seus usuários, mas também ganham vantagem competitiva no mercado global. A governança da cibersegurança deve incentivar investimentos em pesquisa e desenvolvimento (P&D), capacitação de profissionais e colaboração público-privada para criar soluções inovadoras. As tecnologias emergentes, como inteligência artificial aplicada à cibersegurança e à computação quântica, também exigem novos modelos de governança para garantir que sejam desenvolvidas e utilizadas de maneira ética e responsável. Além disso, a sustentabilidade da cibersegurança envolve a criação de incentivos para que pequenas e médias empresas adotem práticas seguras, evitando que apenas grandes corporações tenham os recursos necessários para se protegerem de ameaças cibernéticas.

A governança eficaz da cibersegurança não depende apenas de regulamentos, mas também de um compromisso com transparência e responsabilidade. As empresas que processam dados sensíveis ou operam infraestruturas críticas precisam implementar mecanismos de auditoria de segurança, gestão de riscos e respostas rápidas a incidentes. A adoção de boas práticas de governança corporativa, como a criação de comitês de segurança digital e a publicação de relatórios de conformidade, contribui para um ambiente digital mais seguro e previsível. Além disso, governos devem atuar como facilitadores de um ecossistema de segurança digital confiável, promovendo cooperação internacional, definindo padrões técnicos e incentivando a educação em cibersegurança para que cidadãos, empresas e instituições estejam preparados para enfrentar desafios futuros.

A governança da cibersegurança é um elemento essencial para garantir a estabilidade e o desenvolvimento sustentável do ambiente digital. A crescente interdependência entre sistemas tecnológicos e setores econômicos torna imperativo o fortalecimento de políticas e práticas de segurança robustas, equilibrando proteção, inovação e direitos digitais. A implementação de *frameworks* regulatórios eficazes, aliada à colaboração entre governos, empresas e sociedade civil, será determinante para enfrentar os desafios da cibersegurança nos próximos anos.

5.2.3. Cibersegurança

Até este ponto do capítulo muito se mencionou sobre cibersegurança. Mas, o que é cibersegurança? Esta seção descreve os conceitos principais da cibersegurança e seus princípios, como disponibilidade, integridade, confidencialidade e privacidade. O conceito de cibersegurança tem evoluído ao longo dos anos, expandindo seu foco para além da proteção da informação para abranger um escopo mais amplo de riscos e desafios. Inicialmente, sua abordagem era baseada nos princípios tradicionais de segurança da informação, mas com o avanço da tecnologia, a hiperconectividade e o impacto crescente das ameaças cibernéticas, tornou-se evidente a necessidade de uma visão mais dinâmica e abrangente [Nogueira et al. 2024]. Atualmente, a cibersegurança é vista como uma ciência que estuda e propõe soluções para garantir a segurança do ambiente digital, considerando não apenas aspectos técnicos, mas também fatores humanos, regulatórios e estratégicos. Esse campo tem se beneficiado do avanço de tecnologias emergentes, permitindo respostas mais eficazes contra ameaças cada vez mais sofisticadas.

No passado, a cibersegurança era definida com base nos principais atributos para a segurança da informação, compondo a famosa tríade CIA, em inglês, ***C**onfidentiality*, ***I**ntegrity* e ***A**vailability*, conhecida em português como CID: **C**onfidencialidade, **I**ntegridade e **D**isponibilidade. Com as mudanças nos nossos sistemas, a conexão dos nossos dispositivos, a geração de dados e impacto da cibersegurança nos negócios, empresas, governos e nações, essa definição é considerada limitada e requer um foco maior nas atividades e riscos. Este capítulo e trabalho segue uma visão de cibersegurança como uma ciência. A ciência é uma ferramenta poderosa através da qual nós humanos conseguimos gerar avanços tecnológicos e sociais consideráveis através da aplicação rigorosa do método científico. A ciência representa filosofia, conhecimento e processo. A cibersegurança é um campo recente de pesquisa. Os sistemas digitais datam de menos de 100 anos. As redes de computadores não tem nem 50 anos. Os grandes problemas de segurança não tinham sido observados até as décadas de 1980 e 1990, com o aparecimento e evolução da Internet. Nesses últimos anos, os avanços e a complexidade do ciberespaço cresceram exponencialmente. Brevemente, a cibersegurança é definida como a ciência que estuda e propõe soluções para tornar o ciberespaço seguro contra danos e ameaças, sendo o ciberespaço a integração entre dados, tecnologia e pessoas.

Essa visão mais moderna da cibersegurança engloba diferentes áreas, desde a visão mais técnica, que se expandiu ao longo dos anos com a evolução dos nossos sistemas, até visões voltadas às pessoas, incluindo direito, economia, psicologia, governo, ciências sociais, políticas e outras. Essa visão mais ampla expande as perspectivas da cibersegurança que na definição baseada na tríade CIA trazia limitações por sugerir medidas absolutas, onde um ativo era considerado seguro ou não, o que cria uma falsa sensação de realização, desconsiderando a natureza contínua dos riscos de segurança. Além disso, o foco da tríade incentiva a proteção de ativos individuais em vez de uma abordagem mais ampla e contextual, resultando em soluções temporárias que não abordam o panorama de riscos [Ham 2021]. Para Ham et al. 2021, a tríade não leva em conta o contexto em que os ativos operam, tratando a confidencialidade como uma propriedade isolada, o que pode levar a medidas de segurança ineficazes. Com a evolução da infraestrutura digital e a mudança na natureza das ameaças, é necessário adotar uma abordagem mais dinâmica e contínua para a cibersegurança, em vez de depender de um modelo estático CIA [Lipner and Anderson 2018]. Assim, embora a tríade tenha sido fundamental na cibersegurança, ele não deve mais ser vista como o objetivo final, mas sim como parte de uma atividade contínua que se adapta às mudanças no contexto e nos riscos.

Concomitante à evolução no conceito de cibersegurança, o comportamento dos adversários cibernéticos evoluiu significativamente [de Neira et al. 2020]. Os atacantes agora empregam técnicas avançadas, como engenharia social, *zero day exploits* (*i.e.*, falha ou vulnerabilidade explorada para criar e liberar ameaças antes que os desenvolvedores tenham tempo de criar um pacote para corrigir a vulnerabilidade) e ataques coordenados, tornando a detecção e a resposta mais desafiadoras. Além disso, as motivações por trás dos ataques cibernéticos se diversificaram, abrangendo não apenas ganhos financeiros, mas também objetivos políticos, ideológicos e de espionagem. Essa mudança requer uma compreensão mais abrangente da cibersegurança. A cibersegurança moderna vai além das defesas tradicionais, incorporando estratégias proativas e adaptativas. Essa evolução

inclui a integração da ciência de dados, a inteligência artificial e aprendizado de máquina para detecção de ameaças em tempo real e resposta automatizada [Brito et al. 2023].

Enquanto a tríade CIA estabeleceu a base confidencialidade, integridade e disponibilidade [Lipner and Anderson 2018], a evolução da cibersegurança e a contribuição de diversos especialistas e organizações ao longo dos anos ajudaram a expandir e refinar esses conceitos, incluindo a autenticidade e não repúdio, para atender às necessidades mais complexas da cibersegurança. A **confidencialidade** garante que as informações sensíveis sejam acessíveis apenas para aqueles com autorização, protegendo contra violações de dados e divulgações não autorizadas. A **integridade** assegura a precisão e a confiabilidade dos dados, prevenindo alterações não autorizadas que possam comprometer sua veracidade [Laprie et al. 2004]. A **disponibilidade** garante que as informações e os recursos estejam acessíveis aos usuários autorizados sempre que necessário, protegendo contra interrupções como ataques de negação de serviço. A **autenticidade** confirma que os usuários e os sistemas são genuínos, garantindo que as comunicações e transações sejam feitas por entidades legítimas. O **não repúdio** assegura que uma transação ou comunicação não possa ser negada posteriormente por nenhuma das partes envolvidas, garantindo que as ações realizadas sejam rastreáveis e verificáveis.

Os princípios básicos de segurança aplicados aos sistemas tradicionais, como disponibilidade, integridade, confidencialidade e privacidade, tornam-se ainda mais relevantes no contexto das cidades inteligentes. Isso ocorre devido à grande quantidade de dados sensíveis coletados, processados e distribuídos por dispositivos interconectados, que incluem sensores urbanos, redes de transporte, serviços públicos digitais e infraestruturas críticas. Em geral, essas informações representam dados pessoais, operacionais e administrativos essenciais para o funcionamento dos serviços urbanos. Dessa forma, a disseminação não autorizada desses dados pode acarretar consequências severas para os cidadãos, governos e empresas que operam nesses ecossistemas. A manutenção da privacidade dos dados no escopo de cidades inteligentes apoia-se no uso de *frameworks* robustos que garantam a proteção das informações armazenadas e transmitidas, mantendo-as imunes a manipulações por entidades não autorizadas. A disponibilidade desses dados deve ser assegurada para que entidades autorizadas possam acessá-los conforme necessário.

A cibersegurança de um ecossistema urbano digitalizado é proporcional à proteção de seus elos mais fracos, e os princípios de segurança apresentam relações interdependentes. A Figura 5.4 ilustra que vulnerabilidades em mecanismos de autenticação e controle de acesso podem comprometer a integridade de toda a infraestrutura urbana digital. Nesse contexto, um dos principais desafios é a implementação de soluções de segurança interoperáveis e integradas que contemplem a diversidade de componentes e serviços nas cidades inteligentes. Durante esse processo, deve-se considerar os recursos computacionais disponíveis e as tecnologias aplicáveis para garantir a proteção dos dados. Além disso, as políticas de governança em cibersegurança e privacidade devem atender a regulamentações específicas, que podem variar entre diferentes países e jurisdições. Também é essencial que sejam adotados mecanismos de controle de acesso diferenciados conforme os diferentes níveis de infraestrutura (e.g., borda, névoa e nuvem) e contextos específicos (e.g., resposta a emergências e gestão de desastres naturais). Alguns desses pontos são detalhados a seguir, onde serão explorados os requisitos associados à segurança bem como os principais desafios e práticas adotadas sob a perspectiva das cidades inteligentes.

Figura 5.4: Autenticação e controle em ecossistemas urbanos digitais

Disponibilidade

A cibersegurança e a privacidade dos dados dependem da garantia de disponibilidade das informações e serviços essenciais para organizações, usuários e infraestruturas críticas. A disponibilidade está diretamente relacionada à resiliência dos sistemas conectados, assegurando que falhas em serviços de comunicação, segurança, saúde digital e gestão de energia não comprometam seu funcionamento. Interrupções nesses serviços causam impactos significativos, tornando essencial a adoção de estratégias robustas para mitigar riscos relacionados à disponibilidade. A confiabilidade dos dispositivos IoT, redes de comunicação e infraestruturas em nuvem desempenha um papel central na manutenção da disponibilidade dos serviços. Os dispositivos conectados, como sensores de monitoramento, câmeras de segurança e sistemas de automação, apresentam restrições de energia e capacidade computacional. Dessa forma, os mecanismos de segurança implementados devem equilibrar proteção e eficiência energética. Por exemplo, as técnicas de criptografia devem ser projetadas para reduzir o impacto sobre o consumo energético e a latência dos dispositivos. O monitoramento e a detecção de falhas são fundamentais para garantir a continuidade operacional dos serviços. Sistemas inteligentes podem utilizar aprendizado de máquina para prever e mitigar falhas antes que afetem a infraestrutura. Em dispositivos que transmitem dados periodicamente, interrupções podem indicar falhas operacionais. Já em sistemas que transmitem dados apenas sob condições específicas, o uso de *heartbeats* pode auxiliar na verificação da disponibilidade, exigindo um equilíbrio entre consumo energético e tempo de resposta a falhas.

A segurança dos dispositivos conectados é um desafio crítico, pois o crescimento do número de dispositivos expõe as redes a diversas ameaças cibernéticas. Os ataques de negação de serviço (DoS e DDoS) comprometem a disponibilidade de sistemas essenciais, afetando desde redes corporativas até plataformas de atendimento emergencial. A mitigação desses riscos exige estratégias de detecção e resposta a ataques nos dispositivos de borda e nos roteadores de rede. Medidas como filtragem de tráfego malicioso e bloqueio automático de fontes de ataque são essenciais para a continuidade dos serviços. Além disso, os provedores de nuvem implementam soluções avançadas de mitigação de

DDoS, mas é fundamental adotar políticas de segurança que impeçam que dispositivos comprometidos sejam utilizados como vetores de ataques. Por fim, a resiliência da comunicação requer infraestruturas com redundância de conexões e múltiplos caminhos de transmissão para garantir a continuidade dos serviços. Além disso, a definição de responsabilidades e acordos de nível de serviço para manutenção e resposta a falhas é essencial para evitar interrupções. A gestão da disponibilidade na cibersegurança deve ser parte de um *framework* abrangente, alinhado às melhores práticas e regulamentações, garantindo um ambiente digital seguro e eficiente.

Integridade

A integridade dos dados é um princípio essencial da cibersegurança, garantindo que as informações sejam mantidas íntegras, consistentes e confiáveis ao longo de seu ciclo de vida. A crescente digitalização e o uso de tecnologias como dispositivos IoT e sistemas distribuídos aumentam a complexidade da proteção contra ameaças que podem comprometer a autenticidade e a precisão dos dados. As ameaças à integridade dos dados surgem de diversas formas, incluindo ataques cibernéticos, falhas técnicas e erros operacionais [Brezolin et al. 2024]. Um exemplo crítico é o ataque *Man-in-the-Middle* (MITM), no qual um invasor intercepta e modifica informações trocadas entre sistemas. Além disso, m*alwares* são utilizados para adulterar registros e comprometer a confiabilidade dos dados armazenados. Erros como falhas de *hardware*, configuração inadequada e falta de validação também representam riscos significativos para a integridade dos dados.

Para mitigar essas ameaças, é fundamental adotar práticas e *frameworks* de segurança que fortaleçam a proteção dos dados. Padrões, como a ISO/IEC 27001, fornecem diretrizes para garantir a integridade e segurança da informação. Entre as práticas recomendadas, destacam-se o uso de criptografia e assinaturas digitais, que garantem que os dados não sejam modificados durante a transmissão e que sua origem seja verificável; mecanismos de autenticação e autorização, que promovem um controle rigoroso de acesso para impedir a manipulação não autorizada das informações; detecção de anomalias e monitoramento contínuo, que utilizam inteligência artificial e aprendizado de máquina para identificar padrões suspeitos e possíveis ataques; redundância e validação cruzada de dados, que envolvem a implementação de backups e checagens automatizadas para prevenir a corrupção de informações; e auditorias de segurança, que consistem na revisão periódica de logs e sistemas para detectar possíveis violações e assegurar a integridade dos dados armazenados. Além da implementação de medidas técnicas, é fundamental promover uma cultura organizacional voltada para a cibersegurança, garantindo que usuários e administradores sigam boas práticas e estejam cientes dos riscos envolvidos. Dessa forma, a integridade dos dados pode ser protegida, assegurando maior confiabilidade nos processos e reduzindo vulnerabilidades que possam comprometer a cibersegurança.

Confidencialidade

O princípio da confidencialidade estabelece que informações sensíveis devem ser protegidas contra acessos não autorizados. Em sistemas conectados, como aqueles utiliza-

dos em redes corporativas, dispositivos IoT, aplicações na nuvem e serviços digitais, a confidencialidade garante que dados sigilosos, como credenciais de usuários, registros financeiros e informações pessoais, sejam acessados apenas por entidades autorizadas. A proteção desses dados envolve tanto a segurança na comunicação quanto a segurança no armazenamento, evitando que sejam interceptados, modificados ou utilizados indevidamente. Além disso, medidas eficazes de confidencialidade contribuem para a privacidade dos usuários, dificultando a identificação indevida a partir das informações coletadas. As principais ameaças à confidencialidade ocorrem quando atacantes monitoram e interceptam informações durante a transmissão. Esse tipo de ataque geralmente envolve a captura de dados por meio de monitoramento passivo, seguida da análise do tráfego coletado. Um dos ataques mais comuns nesse contexto é a espionagem, na qual um invasor intercepta comunicações em busca de informações estratégicas. A viabilidade do ataque depende do meio de comunicação utilizado. As tecnologias de curto alcance, como bluetooth, dificultam a interceptação, enquanto redes Wi-Fi, celulares e cabos de dados permitem o monitoramento em larga escala.

Após obter uma quantidade significativa de dados, o invasor pode analisá-los em busca de informações sensíveis. A análise inicial pode incluir a identificação de padrões de tráfego, nomes de usuário e identificadores únicos de dispositivos. Em uma inspeção mais detalhada, o atacante pode correlacionar características específicas para identificar usuários, serviços ou processos automatizados. Caso o invasor consiga mapear comportamentos ou obter credenciais válidas, poderá não apenas comprometer a confidencialidade dos dados, mas também impactar outros princípios de segurança, como integridade e disponibilidade. Além disso, os ataques de personificação ocorrem quando um atacante se passa por um usuário legítimo ou dispositivo autorizado para obter informações continuamente. Nesse cenário, além do vazamento de dados, o sistema pode ser alimentado com informações falsas, comprometendo sua confiabilidade. A proteção da confidencialidade geralmente envolve o uso de criptografia tanto na comunicação quanto no armazenamento de dados. No nível dos dados, mecanismos criptográficos garantem que apenas usuários e sistemas autorizados possam acessá-los. Em ambientes que utilizam computação em nuvem, por exemplo, a criptografia deve ser aplicada antes da transmissão, reduzindo os riscos de exposição durante o transporte e o processamento remoto. No entanto, dispositivos com recursos computacionais limitados, como sensores e sistemas embarcados, exigem soluções de criptografia leve.

Na comunicação segura entre dispositivos e servidores, protocolos como TLS (*Transport Layer Security*) e *IPSec* são amplamente utilizados para estabelecer canais protegidos. Além disso, a escolha do protocolo de comunicação deve considerar recomendações específicas de segurança para mitigar vulnerabilidades inerentes a cada tecnologia. Outra abordagem promissora para garantir a segurança dos dados é o uso de *blockchain*. Essa tecnologia permite o registro imutável das informações em um livro-razão distribuído, reforçando a integridade dos dados. Além disso, contratos inteligentes são utilizados para restringir e controlar o acesso às informações, garantindo a confidencialidade e a privacidade dos dados armazenados. Outro desafio emergente na proteção da confidencialidade é a necessidade de desenvolver soluções de criptografia resistentes à computação quântica. Os algoritmos criptográficos atuais são baseados em problemas matemáticos complexos que não podem ser resolvidos em tempo hábil por computadores

tradicionais. No entanto, espera-se que, com o avanço da computação quântica, algumas dessas proteções se tornem vulneráveis, exigindo novos algoritmos capazes de garantir a segurança dos dados mesmo nesse novo cenário tecnológico [Ribeiro et al. 2023]. Dessa forma, a confidencialidade é um aspecto essencial da segurança da informação em sistemas conectados. O uso de criptografia, protocolos de comunicação seguros e tecnologias emergentes, como *blockchain* e criptografia pós-quântica, são estratégias fundamentais para mitigar ameaças e garantir que informações sensíveis permaneçam protegidas.

Privacidade

A privacidade versa sobre proteger dados sensíveis contra acessos não autorizados e tentativas de exploração indevida. A exposição de informações pessoais resulta em diversos riscos, como vazamento de credenciais, uso indevido de dados para ataques direcionados, extorsão e comprometimento da identidade digital. Além disso, as organizações que falham em proteger a privacidade dos dados enfrentam consequências severas, incluindo perda de credibilidade, danos financeiros e sanções legais. O armazenamento e processamento de informações sensíveis em ambientes digitais são alvos recorrentes de ataques cibernéticos. Para mitigar riscos, é essencial que todos os sistemas implementem mecanismos rigorosos de controle de acesso e autenticação [Nogueira et al. 2021]. Entretanto, a dependência de serviços em nuvem amplia a superfície de ataque, tornando os dados mais expostos e vulneráveis a violações. Além das ameaças externas, existe o risco de exposição intencional total ou parcial de informações por agentes internos que possuem acesso privilegiado. O crescimento do uso de big data e inteligência artificial para análise de informações também requer atenção especial à privacidade. Dados coletados para fins legítimos podem ser reutilizados indevidamente, comprometendo a confidencialidade dos usuários. Empresas e instituições que processam esses dados devem aderir a regulamentações de proteção de dados, como a Lei Geral de Proteção de Dados (LGPD) no Brasil, garantindo transparência sobre a coleta, o uso e a proteção das informações.

Autenticação e Autorização

A autenticação e a autorização são componentes essenciais da cibersegurança, assegurando que apenas usuários e sistemas devidamente identificados possam acessar recursos e serviços digitais. A autenticação consiste em verificar a identidade de uma entidade antes de interagir com sistemas críticos, enquanto a autorização define os privilégios de acesso com base na identidade autenticada. A crescente diversificação de dispositivos conectados e a necessidade de interoperabilidade entre diferentes plataformas tornam a autenticação um desafio contínuo. Métodos tradicionais de autenticação, como senhas, são frequentemente insuficientes diante das ameaças modernas. Como alternativa, soluções mais seguras, como autenticação multifator (MFA), biometria e certificados digitais, têm sido amplamente adotadas para fortalecer a segurança dos acessos.

Entretanto, diversos desafios persistem, incluindo a falta de padronização entre sistemas de autenticação de diferentes fornecedores, a vulnerabilidade de dispositivos com baixa capacidade computacional e a existência de protocolos de comunicação inse-

guros. As tecnologias amplamente utilizadas possuem versões com falhas conhecidas, permitindo que invasores executem ataques para interceptar ou falsificar credenciais. Os principais ataques direcionados a mecanismos de autenticação e autorização incluem falsificação de identidade, clonagem de credenciais, engenharia social e infecção por códigos maliciosos. No ataque por falsificação, um invasor utiliza informações subtraídas de um sistema para se passar por um usuário legítimo e obter acesso indevido a sistemas e dados sensíveis. Os ataques de clonagem envolvem a replicação de credenciais comprometidas para explorar vulnerabilidades em diferentes sistemas.

A engenharia social continua sendo um dos métodos mais eficazes para burlar mecanismos de segurança. Muitos usuários utilizam senhas fracas, reutilizam credenciais ou ignoram práticas recomendadas, facilitando ataques como *phishing*. Além disso, a ausência de autenticação multifator em sistemas críticos aumenta significativamente os riscos. Ataques baseados em códigos maliciosos podem comprometer sistemas inteiros, permitindo que invasores assumam o controle parcial ou total de dispositivos e redes. *Ransomware*, *keyloggers* e *trojans* são algumas das ameaças que podem explorar falhas na autenticação e na autorização para obter acesso não autorizado a sistemas corporativos e redes sensíveis. Para fortalecer a segurança cibernética, é essencial adotar uma abordagem proativa, incluindo o uso de autenticação robusta, monitoramento contínuo de acessos, auditoria de logs e aplicação rigorosa de políticas de segurança. A conscientização dos usuários e a implementação de práticas como a rotação periódica de credenciais e a segregação de privilégios também são fundamentais para reduzir os riscos de ataques cibernéticos e garantir a privacidade dos dados.

Não Repúdio

O princípio do não repúdio assegura que uma transação ou comunicação não possa ser negada posteriormente por nenhuma das partes envolvidas. Esse conceito é fundamental na cibersegurança, pois garante que todas as ações realizadas sejam rastreáveis e verificáveis, proporcionando maior confiabilidade nos processos digitais. Para garantir o não repúdio, diversas técnicas e ferramentas são utilizadas. Entre elas, destacam-se as assinaturas digitais, baseadas em criptografia assimétrica, que asseguram a autenticidade de mensagens e documentos. Além disso, registros auditáveis permitem rastrear atividades em sistemas computacionais, enquanto tokens de autenticação fornecem códigos únicos para validar operações. Esse princípio é essencial em setores como comércio eletrônico, contratos eletrônicos e sistemas bancários, onde a autenticidade e a integridade das transações devem ser garantidas. Ao assegurar que nenhuma das partes possa negar sua participação em uma ação, o não repúdio fortalece a segurança e a confiabilidade dos sistemas digitais.

Vulnerabilidades

Os criminosos cibernéticos buscam constantemente por vulnerabilidades em seus alvos para obter alguma vantagem. Uma vulnerabilidade em um sistema é uma fraqueza no projeto, configuração ou processos que pode ser explorada, comprometendo a segurança. Isso inclui falhas na arquitetura, parâmetros mal configurados ou procedimentos inade-

quados que abrem brechas para ataques. No sistema vulnerável, existe uma oportunidade para uma ameaça quebrar um atributo de segurança (e.g., confiabilidade, disponibilidade, integridade, autenticidade e não repúdio). Quando uma vulnerabilidade é explorada, um invasor pode comprometer o funcionamento de softwares e serviços, roubar identidades e dados pessoais e coordenar ataques contra outros sistemas. Para explorar uma vulnerabilidade de segurança, é necessário um *exploit*, ou seja, uma técnica ou software projetado para se beneficiar de uma vulnerabilidade específica. Existem vários tipos de *exploits*, cada um seguindo diferentes técnicas e propósitos. Por exemplo, o *SQL Injection* é uma técnica onde um invasor insere código SQL malicioso em uma entrada de um aplicativo para manipular ou acessar a base de dados de forma não autorizada. Outro exemplo são os *zero-day exploits*, que visam vulnerabilidades desconhecidas e sem correção disponível.

Ameaças e Atores da Ameaça

Na cibersegurança, uma ameaça representa qualquer potencial perigo de exploração de uma vulnerabilidade para causar danos, perda de dados ou interrupção dos serviços. O ator da ameaça é o indivíduo, grupo, organização ou governo responsável por executar ou planejar um ataque cibernético. O termo adversário é frequentemente utilizado para referenciar qualquer entidade que realiza atividades maliciosas com a intenção de comprometer a segurança de sistemas, redes ou dados. O modelo de adversário descreve as capacidades, objetivos e comportamentos de um atacante em sistemas computacionais ou redes. Ele é essencial na área de segurança, especialmente em criptografia, onde é utilizado para validar a segurança de esquemas e protocolos criptográficos. Um dos modelos mais reconhecidos é o Modelo Dolev-Yao, que assume que um atacante pode escutar toda a comunicação em uma rede e enviar mensagens, mas não pode quebrar a criptografia. Já o Modelo Bellare-Rogaway expande as capacidades do adversário, permitindo modelar diferentes tipos de atacantes, como passivos e ativos. Os vetores de ataque são os métodos ou meios usados por uma ameaça para explorar as vulnerabilidades em sistemas e redes. Entre eles, está o funcionário comprometido, que pode ser manipulado para fornecer acesso não autorizado. A infecção por e-mail ocorre quando mensagens maliciosas induzem usuários a clicar em links ou abrir anexos infectados. O *malware* pode ser introduzido por mídias removíveis, como pen drives, e os dispositivos móveis vulneráveis podem apresentar falhas em aplicativos ou sistemas operacionais.

Um ataque de negação de serviço (do inglês, *Denial of Service*) ou ataque de negação de serviço distribuído (do inglês, *Distributed Denial of Service – DDoS*) utiliza múltiplos meios como vetores de ataques, sendo parte desses vertores de ataques dispositivos conectados para sobrecarregar um alvo. Um bot (diminutivo do inlgês para *robot*) é um dispositivo infectado que executa tarefas programadas, e uma *botnet* é uma redes de dispositivos infectados controlados remotamente por atacantes. Durante um ataque DDoS, um *botmaster* envia comandos para que os bots realizem conexões com a vítima, consumindo seus recursos até causar uma indisponibilidade do serviço.

O *malware* é qualquer software malicioso projetado para explorar vulnerabilidades. Entre os tipos mais comuns estão os vírus, que se anexam a arquivos legítimos e se espalham, e os worms, que se replicam automaticamente em redes. O *adware* exibe anún-

cios indesejados e coleta dados do usuário, enquanto os trojans se disfarçam de software legítimo para roubo de informações. Um *ransomware* é um *malware* que criptografa os dados de um sistema e exige um resgate para a liberação dos dados capturados. *Phishing* é uma técnica de ataque que engana pessoas para que revelem informações pessoais, como senhas e dados financeiros. Ele pode ocorrer por e-mails, SMS e mensagens em redes sociais. O spam refere-se ao envio massivo de mensagens indesejadas, geralmente de caráter publicitário. Muitas vezes, e-mails de spam são usados como vetores para ataques de *phishing*, aumentando as chances de sucesso dos invasores.

5.3. Principais Arcabouços de Governança de Cibersegurança

O crescente avanço das ameaças cibernéticas e a evolução complexa das infraestruturas tecnológicas demandam a implementação de diretrizes que transcendem fronteiras nacionais e setoriais, promovendo uma abordagem coordenada para diminuir ou eliminar vulnerabilidades e assegurar a integridade dos sistemas. Assim, destacam-se os arcabouços amplamente reconhecidos como o do National Institute of Standards and Technology (NIST), os padrões da International Organization for Standardization (ISO) e o modelo de governança de TI promovido pelo Control Objectives for Information and Related Technologies (COBIT).

O NIST, por meio dos arcabouços como o Cybersecurity Framework (CSF), fornece um modelo de gestão de riscos estruturado e adaptável, orientado pela análise de ameaças e respostas às vulnerabilidades emergentes. Por sua vez, os padrões ISO/IEC, notadamente a ISO/IEC 27001 e a ISO/IEC 27002, consolidam diretrizes para a implantação de Sistemas de Gestão de Segurança da Informação (SGSI), estabelecendo um referencial para a conformidade e boas práticas organizacionais. Por fim, o COBIT, desenvolvido pela ISACA, apresenta um modelo abrangente de governança e gestão de TI, alinhando metas corporativas com objetivos de controle e desempenho, com ênfase na responsabilidade organizacional e na melhoria contínua da segurança da informação.

NIST Cybersecurity Framework

O NIST CSF é um arcabouço de avaliação de cibersegurança projetado para analisar a postura cibernética das organizações com base em critérios predefinidos, fornecendo uma metodologia sistemática para identificar pontos fortes, fraquezas e áreas de melhoria nos controles, práticas e processos. Um arcabouço de políticas de cibersegurança, por outro lado, oferece diretrizes estruturadas para os governos locais sobre o que incluir nas políticas de segurança cibernética. As políticas de cibersegurança geralmente não incluem medidas técnicas, mas estabelecem os princípios da governança de segurança cibernética e fornecem uma abordagem estruturada para medidas de segurança voltadas para a prevenção e resposta a ataques cibernéticos [Hossain et al. 2024].

Em fevereiro de 2024, uma década após o lançamento da primeira versão, o Instituto Nacional de Padrões e Tecnologia (NIST) lançou o CSF 2.0, uma atualização do CSF 1.1, publicado em abril de 2018. Até então, o NIST CSF definia os principais pilares de um programa de segurança cibernética eficaz e abrangente por meio de cinco funções essenciais: Identificar, Proteger, Detectar, Responder e Recuperar. Com essa atualização, o NIST introduziu uma sexta função, Governança, que trata de como uma organização pode

tomar e implementar suas próprias decisões internas para fortalecer sua estratégia de segurança cibernética. Essa nova função destaca a cibersegurança como um fator crítico de risco empresarial, equiparando-a a riscos legais, financeiros e outros aspectos estratégicos considerados pela alta liderança. Essas funções são universalmente aplicáveis, permitindo que qualquer organização, independentemente do seu porte ou setor, adapte estratégias para atender aos seus perfis de risco, ambientes tecnológicos e objetivos [Pascoe 2023].

A Figura 5.5 apresenta A Roda de Funções do arcabouço do NIST 2.0. Trata-se de uma ferramenta conceitual usada para representar de forma estruturada as funções de cibersegurança que uma organização deve adotar para gerenciar e mitigar riscos cibernéticos. As funções centrais do arcabouço NIST são os principais componentes que estruturam o arcabouço e orientam as organizações na implementação de práticas eficazes de cibersegurança.

Figura 5.5: Funções do arcabouço NIST 2.0 [Pascoe 2023]

Essas funções são descritas no mais alto nível do arcabouço e são essenciais para criar uma abordagem holística para a segurança cibernética. [Pascoe 2023] define:

- Governar (*GOVERN* - GV) - Estabelecer e monitora as expectativas e a política de gerenciamento de risco de segurança cibernética da organização. A função governar é transversal e fornece resultados para informar como uma organização alcançará e priorizará os resultados das outras cinco funções no contexto de sua missão e expectativas das partes interessadas. Direciona uma compreensão do contexto organizacional; o estabelecimento da estratégia de segurança cibernética e gerenciamento de risco da cadeia de suprimentos de segurança cibernética; funções, responsabilidades e autoridades; políticas, processos, 199 e procedimentos; e a supervisão da estratégia de segurança cibernética.

- Identificar (*IDENTIFY* - ID) - Ajuda a determinar o risco atual de segurança cibernética para a organização. Entender seus ativos (por exemplo, dados, *hardware*,

software, sistemas, instalações, serviços, pessoas) e os riscos de segurança cibernética relacionados permite que uma organização concentre e priorize seus esforços de forma consistente com sua estratégia de gerenciamento de risco e as necessidades de missão 204 identificadas em GOVERNAR.

- Proteger (*PROTECT* - PR) - Usa salvaguardas para prevenir ou reduzir o risco de segurança cibernética. Uma vez que os ativos e riscos são identificados e priorizados, suporta a capacidade de proteger esses ativos para prevenir ou reduzir a probabilidade e o impacto de eventos adversos de segurança cibernética.
- Detectar (*DETECT* - DE) - Encontra e analisa possíveis ataques e comprometimentos de segurança cibernética. Permite a descoberta e análise oportunas de anomalias, indicadores de comprometimento, e outros eventos de segurança cibernética potencialmente adversos que podem indicar que ataques e incidentes de segurança cibernética estão ocorrendo.
- Responder (*RESPOND* - RS) - Toma medidas em relação a um incidente de segurança cibernética detectado. Oferece suporte à capacidade de conter o impacto de incidentes de segurança cibernética.
- Recuperar (*RECOVER* - RC) - Restaura ativos e operações que foram impactados por um incidente de segurança cibernética. Oferece suporte à restauração oportuna de operações normais para reduzir o impacto de incidentes de segurança cibernética e permitir a comunicação apropriada durante os esforços de recuperação.

ISO/IEC 27001

A Organização Internacional para Padronização (ISO) e a Comissão Eletrotécnica Internacional (IEC) estabeleceram a norma ISO/IEC 27001 com o objetivo de fornecer diretrizes e padrões para a governança de sistemas de Tecnologia da Informação (TI). Esse normativo integra a série ISO/IEC 27000, que sistematiza melhores práticas, diretrizes e requisitos técnicos para a proteção de ativos informacionais e a mitigação de riscos organizacionais associados à segurança da informação [Yusif and Hafeez-Baig 2021]. Conforme representado na Figura 5.6, a ISO/IEC 27001 estrutura-se em torno de cinco processos fundamentais: avaliação, direcionamento, monitoramento, comunicação e garantia da segurança dos sistemas de TI. Além disso, define cinco princípios essenciais para a governança de segurança: (i) incorporação da segurança da informação na estrutura organizacional, (ii) adoção de uma abordagem baseada em risco, (iii) criação de um ambiente organizacional seguro, (iv) estabelecimento de diretrizes para investimentos em segurança da informação e (v) revisão e avaliação do desempenho com base nos resultados estratégicos da organização.

Adicionalmente, a ISO/IEC 27001 fornece um referencial normativo para a integração e o alinhamento das estratégias de TI com os objetivos estratégicos da organização. O modelo de governança proposto abrange os níveis estratégico, tático e operacional, fornecendo mecanismos para o direcionamento, monitoramento e avaliação das funções e atividades relacionadas à segurança da informação no contexto corporativo. Entretanto, a adoção da ISO/IEC 27001 apresenta desafios significativos. Entre as principais limitações, destaca-se a complexidade inerente ao seu processo de implementação, que exige

conformidade com extensas listas de verificação e requisitos normativos voltados à auditoria e à certificação. Esse fator gera resistência organizacional, dado o alto custo associado à adoção do padrão, bem como a necessidade de especialistas altamente qualificados em segurança da informação e governança de TI. Além disso, a implementação demanda recursos substanciais em termos de tempo, infraestrutura e capacitação profissional, o que pode dificultar sua adoção em organizações com restrições orçamentárias ou baixa maturidade em governança da segurança da informação.

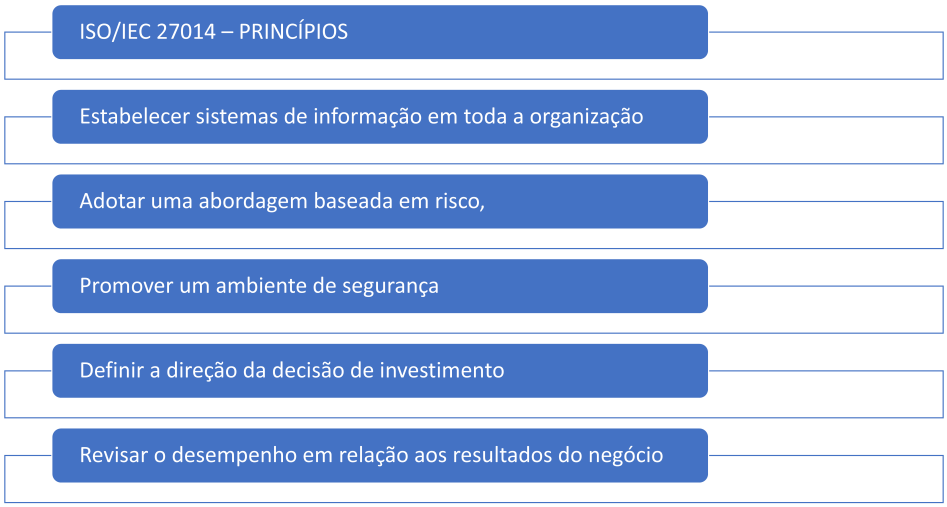

Figura 5.6: ISO/IEC 27001 - Princípios de governança

COBIT 2019

O COBIT (*Control Objectives for Information and Related Technologies*) é uma estrutura voltada para a governança e gestão da tecnologia da informação nas organizações. A versão mais recente, COBIT 2019, sucedeu à COBIT 5 e representa a sexta edição lançada pela ISACA *(Information Systems Audit and Control Association)*. Essa atualização trouxe uma série de aprimoramentos na arcabouço de governança, incluindo a introdução de seis princípios de governança, a definição de 40 processos que estruturam a gestão da TI, a adição de novos princípios à estrutura de governança, a incorporação de fatores de desenho que permitem adaptar a estrutura às necessidades específicas de cada organização, além da renomeação dos *enablers* (facilitadores) para componentes.

Além disso, o COBIT 2019 foi desenvolvido com base em dois princípios principais. Um que apresenta os principais requisitos do sistema governamental e um segundo - do sistema de governança, que são usados para construir o sistema de governança para organizações. Há também três princípios para uma estrutura de governança; a estrutura de governança deve ser baseada em um modelo conceitual, aberto e flexível, e alinhada com outros regulamentos, estruturas e padrões. Conforme ilustra a Figura 5.7, adaptada de [Information Systems Audit and Control Association 2018], são seis os princípios indicados para um sistema de governança. Entretanto, COBIT 2019 foi desenvolvido com

Figura 5.7: Princípios Sistema de Governança - COBIT 2019

base em dois conjuntos de princípios: Princípios para um Sistema de Governança e princípios de uma arcabouço de Governança, que são utilizados para construir um sistema de governança para organizações. Existem também três princípios para um arcabouço de Governança - Baseado no modelo conceitual, Aberto e flexível e Alinhado aos principais padrões.

Os seis princípios direcionam a definição de um sistema de governança da informação e tecnologia nas organizações, conforme estabelecido pela ISACA no arcabouço COBIT 2019 [Information Systems Audit and Control Association 2018]. Esse seis princípios são descritos a seguir.

Fornecer valor às partes interessadas: cada instituição precisa de um sistema de governança para satisfazer as necessidades dos atores envolvidos e para gerar valor a partir do uso da Tecnologia da Informação.

Abordagem holística: um sistema de governança para a informação e tecnologia (I&T) nas organizações é construído a partir de diversos componentes, que podem ser de diferentes tipos e que funcionam em conjunto de forma holística, a qual pressupõe a consideração do sistema como um todo, valorizando as inter-relações entre seus elementos em detrimento de análises fragmentadas ou isoladas.

Sistema de governança dinâmico: um sistema de governança deve ser dinâmico. Isso significa que, sempre que um ou mais fatores de projeto forem alterados, o impacto dessas mudanças no sistema de governança e gestão da informação e tecnologia deve ser considerado.

Distinguir governança e gestão: O COBIT diferencia claramente os conceitos de governança (responsável por avaliar, direcionar e monitorar) e gestão (responsável por planejar, construir, operar e monitorar). Essa distinção ajuda a estabelecer papéis, responsabilidades e mecanismos de controle adequados.

Adaptar-se às necessidades da organização: O sistema de governança deve ser customizável, ou seja, adaptado ao contexto específico de cada organização — considerando seu porte, setor, cultura, perfil de riscos e objetivos estratégicos. Essa flexibilidade permite maior efetividade na aplicação do arcabouço.

Sistema de governança de ponta a ponta: A governança deve abranger toda a organização, incluindo todas as funções e processos relevantes de I&T. Vai além da função de TI tradicional, envolvendo todas as áreas que utilizam ou gerenciam informações e tecnologias.

Conforme citado, de acordo com o padrão COBIT 2019, existem três princípios essenciais que devem orientar a estruturação de um arcabouço de governança. Esses princípios são ilustrados na Figura 5.8, adaptada de [Information Systems Audit and Control Association 2018].

- Um arcabouço de governança deve ser baseado em um modelo conceitual, identificando os componentes-chave e os relacionamentos entre esses componentes, para maximizar a consistência e permitir automação.

- Um arcabouço de governança deve ser aberto e flexível. Ele deve permitir a adição de novos conteúdos e a capacidade de abordar novas questões da forma mais flexível possível, mantendo a integridade e a consistência.

- Um arcabouço de governança deve estar alinhado aos principais padrões, arcabouços e regulamentos relacionados.

Apesar de sua ampla adoção, o COBIT 2019 apresenta limitações práticas relevantes. Entre os principais desafios estão a complexidade conceitual e estrutural, a ausência de diretrizes claras para a implementação e a carência de evidências que comprovem seus benefícios. O arcabouço possui foco predominante em sistemas de TI, não abordando de forma abrangente questões relacionadas à cibersegurança. Outro fator limitante é o alto custo de implementação, o que inibe sua adoção por organizações com recursos limitados ou com baixo nível de maturidade em segurança da informação. A exigência elevada de conhecimento técnico e de profissionais especializados, bem como a necessidade de treinamento intensivo, também representam barreiras à sua aplicabilidade. Embora seja amplamente reconhecido como um modelo de governança de TI, o COBIT configura-se, na prática, como um arcabouço de gestão voltado à resolução de problemas organizacionais [Melaku 2023].

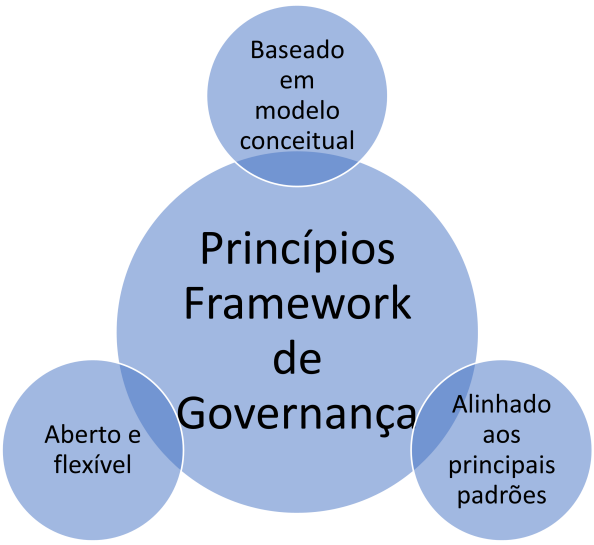

Figura 5.8: Princípios arcabouço Governança - COBIT 2019

Comparação arcabouços de governança

No cenário cidades inteligentes, a relação entre sistemas urbanos e tecnologias digitais demanda estruturas de governança em cibersegurança e privacidade dos dados. À medida que sensores, redes e plataformas inteligentes passam a integrar serviços públicos urbanos, torna-se fundamental adotar um arcabouço que oriente a gestão da informação, da comunicação e dos sistemas de uma forma geral. As Tabelas 5.1 e 5.2, adaptadas de [Melaku 2023], apresentam uma análise comparativa entre os principais arcabouços utilizados globalmente para esse fim — COBIT, ISO/IEC 27001 e NIST — considerando aspectos como definição, função, aplicabilidade, foco, requisitos de certificação e escopo. Essa comparação visa apoiar a escolha de abordagens estratégicas para a construção de ambientes urbanos digitais seguros.

A análise comparativa revela que cada arcabouço contribui de forma distinta para a governança da cibersegurança e da privacidade em cidades inteligentes. O COBIT oferece uma abordagem estruturada voltada à alta gestão, com ênfase em auditoria e conformidade. O ISO/IEC 27001, destaca-se pela formalização de práticas e pela busca de certificações, sendo particularmente útil para organizações que desejam validar seus processos perante padrões internacionais. O arcabouço do NIST, amplamente adotado em ambientes críticos, proporciona uma base flexível para a avaliação de riscos e o fortalecimento da resiliência cibernética. A adoção estratégica — ou mesmo combinada — desses modelos pode representar um diferencial significativo na implementação de uma governança eficaz da informação nas cidades inteligentes.

Tabela 5.1: Tabela de comparação entre arcabouços de governança (Parte 1)

Parâmetros	**COBIT**	**ISO/IEC**	**NIST**
Definição	Estrutura de negócios e melhores práticas para sistemas de TI de governança e gestão.	Um padrão internacional para o gerenciamento de serviços fornecidos por sistemas e requisitos de TI.	Uma estrutura voluntária baseada em padrões, diretrizes e práticas existentes para melhorar a gestão de riscos de cibersegurança em sistemas de informação.
Função	Ele define um conjunto de padrões e requisitos para governança, gerenciamento e controle de sistemas e processos de TI.	Ele define um conjunto de padrões e requisitos para a formação, implementação, manutenção e melhoria contínua da segurança cibernética.	Fornecer um guia para identificar, proteger, detectar, responder e recuperar frente a ameaças de cibersegurança.
Requisito de certificação	A implementação não requer certificação.	A implementação requer certificação.	A implementação não requer certificação obrigatória. O arcabouço é voluntário e adaptável.
Aplicabilidade	É aplicável a qualquer tipo e tamanho de organização. É frequentemente usado pela alta gerência que é responsável por conformidade e auditoria.	É aplicável a qualquer tipo e tamanho de organização. É frequentemente usado por organizações suportadas por TI que querem provar que estão em conformidade com as melhores práticas e padrões definidos externamente.	Pode ser adotado por qualquer organização, pública ou privada, independentemente do porte, com foco especial em infraestrutura crítica.
Foco	Focado em auditoria e conformidade. Versões recentes focadas em governança e gerenciamento de serviços de TI.	ISO/IEC focada em atender aos requisitos de certificação para validar a conformidade com os padrões.	Foco na gestão de riscos cibernéticos, proteção de ativos e continuidade de negócios.

Tabela 5.2: Tabela de comparação entre arcabouços de governança (Parte 2)

Parâmetros	**COBIT**	**ISO/IEC**	**NIST**
Domínio/Área	40 processos e quatro domínios	Mais de dez domínios	Cinco funções principais: Identificar, Proteger, Detectar, Responder, Recuperar.
Implementação	Auditoria de sistemas de informação	Gerenciamento de nível de serviço de Sistemas de informação	Avaliação de maturidade e criação de planos de ação para cibersegurança
Usado principalmente para	Descrever os requisitos de auditoria e conformidade para Sistemas de TI	Demonstrar que a organização de TI atende a um conjunto adequado de padrões e melhores práticas	Avaliar e aprimorar a postura de cibersegurança de uma organização
Emissor	ISACA	ISO/IEC, Tecnologia da Informação, Subcomissão SC 27, Segurança da informação, segurança cibernética e proteção da privacidade, integração com ITU-T SG 17	NIST (EUA), com apoio de stakeholders públicos e privados

5.4. Estado da Arte

Uma Revisão Sistemática da Literatura (RSL) foi conduzida para investigar as principais soluções de governança de cibersegurança para cidades inteligentes, com o objetivo de identificar desafios e práticas relevantes para a proteção e gestão de dispositivos IoT no contexto tratado. A RSL é um método de estudo que emprega estratégias para selecionar, analisar, avaliar e resumir artigos de um banco de dados sobre o tema, a fim de obter uma investigação consistente do tema e até mesmo fornecer orientações para pesquisas futuras. O protocolo de pesquisa selecionado para este estudo baseia-se na metodologia PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analysis*) [Takkouche and Norman 2011] e busca responder às seguintes questões:

- Quais são os principais arcabouços de governança em cibersegurança citados ou utilizados para a proteção e gestão de dispositivos IoT em cidades inteligentes?
- Quais são os principais desafios descritos pelos trabalhos selecionados?
- Quais as principais lacunas sobre governança de cibersegurança?
- O arcabouço proposto (ou citado) é validado ou implementado? Se sim, como é validado ou implementado?
- Quais são as principais tecnologias citadas para apoiar a implementação do arcabouço?

Com o objetivo de avaliar pesquisas mais recentes, essa revisão limitou-se aos trabalhos publicados a partir de 2020. Além disso, a RSL incluiu bases de dados significativas na área de Tecnologia da Informação, incluindo *Science Direct*, *IEEE Xplore*, e *Scopus*. Os estágios do método de pesquisa, as palavras-chave de buscas, bem como o encadeamento lógico utilizado, são apresentados na Figura 5.9. A pesquisa, realizada em março de 2025, retornou um total de 245 artigos, conforme apresentado na Figura 5.9. Após a leitura do título e resumo, 173 artigos que não tinham relação com os critérios de inclusão foram excluídos. Após isso, 1 artigo duplicado foi excluído e 71 artigos permaneceram para leitura completa. Os critérios de elegibilidade incluíram artigos que se concentravam em governança no contexto de cidades inteligentes e *IoT*. Então, após a avaliação do texto completo, 65 artigos foram excluídos por não serem relevantes para o objetivo da revisão. No final, restaram 6 artigos para revisão final. Uma breve apresentação dos artigos selecionados é apresentada a seguir. Logo após, cada pergunta de pesquisa é respondida com base nos achados de cada artigo.

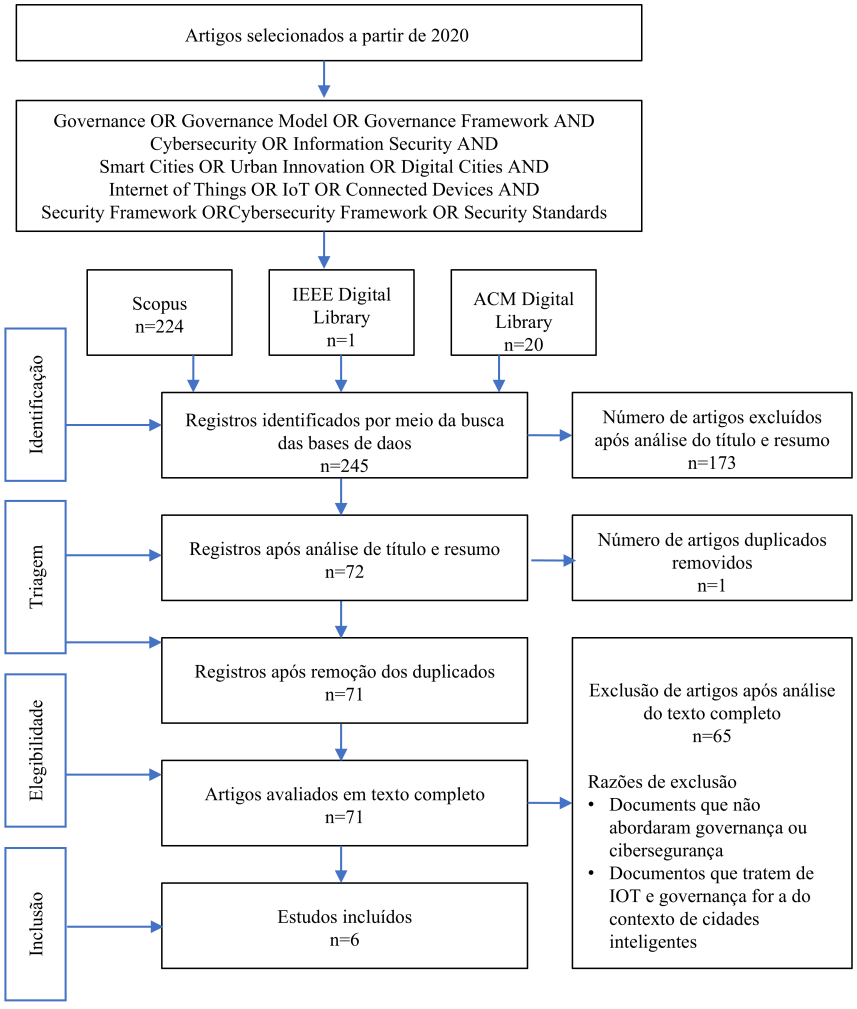

Figura 5.9: Diagrama de Fluxo PRISMA do processo de seleção de artigos

- [Siddiqui et al. 2024] apresenta uma arquitetura de governança adaptativa de segurança baseada em contratos inteligentes para a interoperação de serviços em cidades inteligentes. A pesquisa explora o uso de *blockchain multi-chain*, Redes Definidas por *Software* (SDN) e APIs de serviços inteligentes para fortalecer a segurança cibernética e a proteção da privacidade. O artigo enfatiza a necessidade de *frameworks* regulatórios para mitigar riscos decorrentes da hiperconectividade urbana, garantindo a transparência e a eficiência administrativa.

- O trabalho de [Hossain et al. 2024] examina políticas de segurança cibernética adotadas por governos locais, utilizando o NIST Cybersecurity Framework 2.0 como referência. A pesquisa identifica vulnerabilidades em infraestruturas públicas digitais e propõe diretrizes para aprimorar a resiliência contra ameaças cibernéticas. O artigo está voltado à implementação de *frameworks* regulatórios e estratégias de governança para proteger serviços urbanos essenciais.

- Em [Sedrati et al. 2022], os autores propuseram um *framework* de governança de *IoT* estruturado em três camadas, empregando *blockchain* para descentralização e segurança. O estudo é validado por meio de um caso de uso em um sistema de estacionamento inteligente, demonstrando a viabilidade de uma abordagem distribuída para gestão de infraestruturas urbanas.

- Em [Yuliana and Hasibuan 2022], os autores discutem a criação de um *framework* de governança de segurança da informação para governos digitais. A pesquisa enfatiza a necessidade de uma abordagem padronizada para garantir compatibilidade entre diferentes sistemas, evitando fragmentações que comprometam a segurança e a eficiência operacional.

- O trabalho de [Buckwald and Marchant 2021] explora a governança da *IoT* por meio de abordagens baseadas em *soft law*. *Soft low* é um termo usado para descrever instrumentos quase legais que, embora não sejam legalmente executáveis, ainda podem exercer influência e moldar o comportamento. A pesquisa analisa como princípios de privacidade por design e soluções de *blockchain* podem ser aplicadas para aumentar a segurança e a confiabilidade das infraestruturas *IoT*. Destaca a importância de normativas flexíveis que se adaptem às inovações tecnológicas.

- O trabalho apresentado em [Rao and Deebak 2023] aborda a segurança e a privacidade em ambientes *IoT* para cidades inteligentes e indústrias. A pesquisa discute autenticação, gerenciamento de chaves e protocolos de proteção de dados, ressaltando como tais tecnologias podem fortalecer a resiliência cibernética.

A análise dos artigos revela que a governança da cibersegurança e da privacidade na *IoT* depende de uma abordagem integrada, que combina regulamentação, inovação tecnológica e conscientização social. A seguir, as questões de pesquisa são respondidas a partir da análise de cada um dos artigos selecionados:

5.4.1. Quais são os principais arcabouços de governança em cibersegurança citados ou utilizados nos artigos para a proteção e gestão de dispositivos IoT em cidades inteligentes?

O NIST Cybersecutity Framework, NIST 800-162, COBIT, ISO 27001 e ITIL foram encontrados nos trabalhos selecionados, conforme descrito a seguir. O NIST Cybersecutity Framework 2.0 (CSF 2.0) é empregado como base para avaliar a eficácia das políticas de cibersegurança adotadas por governos locais no trabalho de [Hossain et al. 2024]. O NIST Cybersecutity Framework, mas na versão 1.0, é citado no trabalho de Sedrati et al. ao se referir a um dos trabalhos relacionados [Sedrati et al. 2022]. O trabalho de Webb e Hume descreve a iniciativa de uma universidade dos EUA que adotou o NIST Cybersecurity Framework combinado com um novo modelo de governança de segurança da informação para permitir à Universidade implementar um campus inteligente com soluções *IoT* envolvendo transporte inteligente, estacionamento inteligente e a implantação de uma rede *LoRaWAN* para apoiar projetos de pesquisa do corpo docente [Webb and Hume 2018]. Sedrati *et al.* ainda citam o ITIL ao se referir em *frameworks* estabelecidos para governança de TI que foram estendidos e/ou adaptados para contextos IoT. O trabalho de [Rao and Deebak 2023] cita uma publicação especial do NIST (800-162) voltada ao controle de acesso baseado em atributos, também do NIST. A discussão gira em torno da arquitetura em camadas da *IoT*, apresentando os requisitos de segurança e os protocolos associados a cada camada, como a de percepção, rede, serviço e aplicação. O trabalho não descreve um modelo formal de governança, mas sim práticas e mecanismos técnicos com potencial de aplicação em um *framework* de governança.

O COBIT é citado em [Sedrati et al. 2022] e [Yuliana and Hasibuan 2022]. Destaque para o trabalho de Yuliana e Hasibua que afirma que tanto o COBIT 5 quanto o padrão 27001:2013 são geralmente usados para analisar o nível de maturidade dos sistemas de segurança da informação da Indonésia. O ISO 27001 também é citado no trabalho de Sedrati *et al.*. O trabalho de [Buckwald and Marchant 2021] não cita especificamente algum *framework*, mas afirma que dentre os principais *frameworks* estão os padrões desenvolvidos por consórcios e organizações de padronização como a ISO e o IEEE. O artigo de [Hossain et al. 2024] propõe implementar um *framework* adaptativo de governança para lidar com segurança e interoperabilidade em cidades inteligentes usando tecnologias como SDN e *blockchain*.

5.4.2. Quais são os principais desafios descritos pelos trabalhos selecionados?

A falta de padronização e a dificuldade de interoperabilidade entre dispositivos e serviços são apontadas por alguns autores dos trabalhos selecionados. [Siddiqui et al. 2024] apontam a falta de padrões sintáticos comuns entre os diferentes serviços urbanos. [Sedrati et al. 2022] apontam a diversidade e quantidade de dispositivos *IoT*, que acabam gerando problemas de interoperabilidade e de escalabilidade. [Rao and Deebak 2023] reforçam a preocupação com a falta de padronização nos protocolos de comunicação e segurança como um dos principais desafios.

Outro ponto recorrente entre os autores é a limitação técnica dos próprios dispositivos. [Sedrati et al. 2022] alertam para os riscos de segurança e privacidade em dispositivos com recursos limitados, como processamento e armazena-

mento. [Buckwald and Marchant 2021] observam que esses dispositivos têm pouca ou nenhuma proteção, o que os torna alvos para ataques. [Rao and Deebak 2023] mencionam uma série de ameaças, como DoS, *spoofing*, ataques do tipo *man-in-the-middle* e injeções de dados falsos, ressaltando a dificuldade de aplicar medidas de proteção que sejam ao mesmo tempo eficazes e leves o suficiente para esses dispositivos mais simples.

A ausência de soluções adaptativas e escaláveis também é motivo de preocupação. [Siddiqui et al. 2024] destacam a carência de mecanismos de segurança que consigam se ajustar automaticamente a novas ameaças e a ambientes em constante mudança. Eles também mencionam a baixa escalabilidade de sistemas baseados em *blockchain* e os riscos de falhas em arquiteturas SDN tradicionais, além da dificuldade de coordenar múltiplos serviços com diferentes exigências técnicas e legais.

Vários autores também chamam atenção para os desafios de natureza regulatória e organizacional. [Siddiqui et al. 2024] ressaltam a importância de garantir conformidade com normas legais e regulatórias, enquanto [Sedrati et al. 2022] abordam questões ligadas à responsabilidade no uso e compartilhamento de dados, além da falta de *frameworks* de governança que sejam amplos e flexíveis o suficiente para diferentes contextos. [Buckwald and Marchant 2021] acrescentam a ausência de um arcabouço regulatório robusto, a fragmentação de padrões e o descompasso entre o avanço tecnológico e a lentidão das respostas legislativas. Já [Yuliana and Hasibuan 2022] focam nos desafios enfrentados pelo governo da Indonésia, como a fragmentação entre setores, a falta de políticas claras, a baixa maturidade dos sistemas de segurança e a escassez de capacitação entre os profissionais da administração pública.

5.4.3. Quais as principais lacunas sobre governança em cibersegurança descritas nos artigos?

Em sua análise dos *frameworks* existentes [Sedrati et al. 2022] revelou lacunas relevantes. A primeira é o foco excessivo em objetivos de negócios, o que resulta em uma governança voltada para atores humanos, com pouca ou nenhuma ênfase nos dispositivos enquanto agentes decisórios. Também se verifica a ausência de modelos que permitam a tomada de decisão descentralizada, fundamental em sistemas distribuídos como os da *IoT*. Outro ponto negligenciado nos frameworks analisados são os princípios democráticos de governança, como transparência, equidade, prestação de contas e participação aberta, que são centrais especialmente em ambientes urbanos e públicos.

A principal lacuna apontada por [Buckwald and Marchant 2021] refere-se à falta de leis e regulamentos específicos que lidem de forma abrangente com os riscos à segurança e privacidade no contexto da *IoT*. Também destaca-se a inexistência de diretrizes oficiais para garantir práticas mínimas de segurança e privacidade, bem como a falta de mecanismos robustos de responsabilização e transparência por parte das empresas que desenvolvem e operam dispositivos *IoT*. De maneira complementar, em [Rao and Deebak 2023], identificam-se como as principais lacunas a ausência de um modelo integrado que assegure a interoperabilidade entre dispositivos e sistemas de diferentes fabricantes e arquiteturas. Destaca-se a inexistência de mecanismos padronizados de autenticação e privacidade que sejam amplamente adotados no contexto urbano e industrial. O artigo de [Hossain et al. 2024] identifica como principais lacunas a ausência

de políticas de cibersegurança específicas para o contexto de cidades inteligentes e a desatualização de muitos documentos normativos dos governos locais. Também, aponta-se a falta de mecanismos consistentes para o monitoramento contínuo, auditoria e atualização das políticas, que compromete a eficácia frente à rápida evolução das ameaças e tecnologias digitais.

5.4.4. O arcabouço proposto ou citado é validado ou implementado? Se sim, como é validado ou implementado.

O framework citado (NIST CSF 2.0) por [Hossain et al. 2024] é utilizado como ferramenta de avaliação, mas não é implementado nem validado no contexto prático pelos governos locais analisados. Por sua vez, o artigo propõe um novo *framework* de política de cibersegurança específico para governos locais, composto por sete componentes principais e 38 subitens, que incluem desde a introdução do documento e governança organizacional até protocolos para trabalho remoto e segurança em cidades inteligentes. No entanto, esse *framework* proposto também não foi validado ou implementado. Ele é apresentado como uma sugestão teórica e estruturada, e destina-se a orientar futuras formulações, mas não passou por testes ou aplicações práticas até o momento da publicação.

A proposta de [Sedrati et al. 2022] é uma das efetivamente testadas em um cenário realista, ainda que em ambiente controlado. A prova de conceito foi implementada em um hospital público, demonstrando a aplicação do modelo de governança com base em controle de acesso (ABAC) mediado por contratos inteligentes na *blockchain Ethereum*. Os testes de desempenho comprovaram a viabilidade técnica em termos de consumo de recursos, apontando em direção à aplicação prática da governança descentralizada de dispositivos IoT. O framework proposto no artigo [Yuliana and Hasibuan 2022] foi desenvolvido por meio de uma abordagem metodológica estruturada em três etapas: (1) construção inicial com base no modelo de governança de sistemas ciberfísicos e fatores críticos de sucesso da segurança da informação; (2) *benchmarking* internacional com *frameworks* de segurança de países como Estados Unidos, Malásia e Nigéria, para validar a aplicabilidade dos componentes selecionados; e (3) complementação com parâmetros, elementos e recomendações específicas ao contexto indonésio, criando um modelo adaptado à realidade local. Embora não tenha sido validado empiricamente em um ambiente de governo real, o *framework* foi fundamentado em uma revisão bibliográfica ampla e comparação com práticas internacionais. Os autores destacam a necessidade de validações futuras para a implementação das atividades concretas nos subcomponentes identificados.

5.4.5. Quais são as principais tecnologias citadas para apoiar a implementação do arcabouço?

Os trabalhos analisados apresentam diferentes níveis de detalhamento em relação às tecnologias e mecanismos utilizados para apoiar a implementação de *frameworks* de cibersegurança em cidades inteligentes. Em alguns casos, como no artigo de [Hossain et al. 2024], não há a indicação de ferramentas ou soluções específicas. Os autores mencionam, de forma geral, a importância de práticas como monitoramento contínuo, autenticação, controle de acesso, *backups* e criptografia, além de citarem tecnologias emergentes como OSINT (*Open Source Intelligence*) e IoTSE (*Internet of Things Security Exploits*) como tendências para avaliação de vulnerabilidades. No entanto, o texto

se mantém em um nível conceitual, sem abordar diretamente plataformas, *softwares* ou dispositivos aplicados pelos governos locais.

Por outro lado, outros estudos oferecem descrições mais técnicas e detalhadas. [Siddiqui et al. 2024] propõem uma arquitetura baseada em contratos inteligentes e redes definidas por software (SDIoT), com destaque para o uso do *MultiChain 2.0* em um ambiente descentralizado. Os contratos, escritos em *Python*, automatizam a aplicação das regras de segurança. A arquitetura é complementada pelo uso do SDN-WISE como controlador de rede e pela criptografia de curvas elípticas (ECC), utilizada para garantir trocas de dados seguras entre os nós da rede. De forma semelhante, o *framework* apresentado por [Sedrati et al. 2022] foi implementado e validado por meio de uma prova de conceito aplicada a um estacionamento inteligente. A proposta combina um modelo de controle de acesso baseado em atributos (ABAC), contratos inteligentes executados na *blockchain Ethereum* e o uso de *Raspberry Pi* como hubs para autorizações em dispositivos com restrições computacionais. A implementação também envolveu testes de desempenho, que avaliaram o consumo de memória e processamento, demonstrando a viabilidade do modelo em ambientes com recursos limitados.

Outros trabalhos, como o de [Buckwald and Marchant 2021], enfatizam abordagens voltadas à segurança desde a concepção dos sistemas, com foco na arquitetura de *privacy and security by design*. Essa abordagem inclui mecanismos como criptografia, pseudonimização, autenticação, limitação da coleta de dados e atualizações de segurança. O uso de *blockchain* também é citado como uma tecnologia promissora para assegurar integridade, controle e privacidade dos dados gerados por dispositivos *IoT*. Por fim, [Rao and Deebak 2023] apresentam um conjunto variado de tecnologias voltadas à proteção da segurança e privacidade, incluindo algoritmos criptográficos como RSA, AES, ECC e SHA, e diferentes formas de autenticação (simples, dupla e multifatorial). Eles também destacam o uso combinado de computação em nuvem, em borda (*edge computing*) e em névoa (*fog computing*) como arquiteturas complementares para gestão segura dos dados.

A Tabela 5.3 oferece uma visão dos principais aspectos abordados nos seis artigos selecionados, proporcionando uma visão sintetizada das contribuições dos trabalhos e uma análise comparativa das abordagens adotadas. Essa comparação abrange os *frameworks* de governança mencionados, os desafios descritos, as lacunas identificadas, a validação ou implementação dos modelos propostos, e as tecnologias destacadas em cada estudo. Através dessa tabela, é possível observar as semelhanças e diferenças entre os trabalhos, além de entender como os pesquisadores abordam as questões centrais da segurança cibernética no contexto das cidades inteligentes.

Tabela 5.3: Comparação entre os artigos selecionados

Artigo	***Frameworks* citados ou utilizados**	**Desafios identificados**	**Lacunas apontadas**	**O *framework* é validado?**	**Tecnologias de apoio**
Hossain et al. (2024)	NIST CSF 2.0 (como base); proposta de novo *framework* para governos locais	Falta de políticas específicas para cidades inteligentes; políticas vagas ou desatualizadas	Ausência de foco em cidades inteligentes; falta de mecanismos de atualização e monitoramento	Não; *framework* teórico	Criptografia, *backup*, autenticação, OSINT, IoTSE (sem detalhamento técnico)
Sedrati et al. (2022)	NIST, ISO 27001, ITIL, COBIT (referenciados e adaptados); novo *framework IoT-Gov*	Escalabilidade, interoperabilidade, segurança em dispositivos com poucos recursos, lacunas legais	Modelos focados em humanos e negócios; falta de descentralização e princípios democráticos	Sim; validado com prova de conceito em hospital público	*Blockchain Ethereum*, ABAC, contratos inteligentes, *Raspberry Pi*, sensores e câmeras com restrições
Buckwald et al. (2021)	*Soft law*; padrões ISO, IEEE; boas práticas; privacidade e segurança por *design*	Vulnerabilidade de dispositivos; coleta massiva de dados; ausência de responsabilização; fragmentação de padrões	Falta de leis e diretrizes específicas; ausência de transparência e responsabilização	Não; discussão teórica	Criptografia, pseudonimização, *blockchain*, segurança por design, atualização de *firmware*
Siddiqui et al. (2024)	*Framework* adaptativo com contratos inteligentes e SDIoT	Falta de padrões comuns; baixa escalabilidade da *blockchain*; falhas em SDN; desafios regulatórios	Implícitas nos desafios técnicos; não abordadas formalmente como lacunas	Sim; validado com simulações e protótipos em *Python*	*MultiChain 2.0*, *blockchain*, SDIoT, SDN-WISE, contratos inteligentes (*Python*), ECC
Rao et al. (2023)	Não apresenta *framework*; usa abordagem por camadas da IoT	Dispositivos vulneráveis; ataques (DoS, *spoofing*, etc.); ausência de padrões; dificuldade de integração	Ausência de modelo integrado; falta de padrões amplamente adotados	Não	RSA, AES, ECC, SHA, autenticação multifatorial, *cloud/edge/fog computing*, MQTT, CoAP, Zigbee, LoRaWAN, BLE, *machine/deep learning*
Yuliana & Hasibuan (2022)	*Framework* próprio baseado em COBIT 5, ISO 27001 e outros	Fragmentação da segurança na governança pública; ausência de diretrizes integradas e contínuas	Falta de alinhamento entre TI e segurança da informação; carência de atividades práticas	Não; proposta teórica com *benchmarking* e análise de lacunas	Não menciona tecnologias específicas

5.5. Estudo de Caso

Essa seção apresenta um estudo de caso sobre a aplicação de *frameworks* de governança da informação e tecnologia em redes elétricas inteligentes (*Smart Grids*), no contexto das cidades inteligentes. A proposta é analisar como estruturas como o COBIT 2019, a ISO/IEC 27001 e o NIST Cybersecurity Framework podem ser usadas para garantir segurança, confiabilidade e alinhamento estratégico na gestão desses sistemas críticos. O estudo aborda os principais desafios de segurança, os pontos fortes e fracos de cada *framework* e propõe um modelo integrado de governança voltado à sustentabilidade e à eficiência urbana

5.5.1. Governança de cibersegurança aplicada a *Smart Grids*

Com o avanço das cidades inteligentes, a integração entre infraestrutura urbana e tecnologias digitais se tornou essencial, entretanto estudos sobre governança e gerenciamento de cibersegurança são praticamente desconhecidos, especialmente no que diz respeito ao setor energético [Pardini et al. 2017]. Uma das inovações mais estratégicas nesse cenário é a *Smart Grid*, ou rede elétrica inteligente, que representa uma transformação na forma como a energia elétrica é gerada, distribuída e consumida. Consistem na implementação do uso da informação digital e controle de tecnologia para melhorar a confiabilidade, a segurança e a eficiência da rede elétrica [Kassakian et al. 2011].

A estrutura crítica analisada é o centro de operações de energia de uma cidade hipotética com uma rede elétrica inteligente implementada. Essa rede conta com medidores inteligentes (*smart meters*), dispositivos *IoT* conectados à rede elétrica e sistemas de análise preditiva para identificação de falhas. A operação dessa estrutura depende de uma comunicação contínua e integrada entre os elementos físicos (transformadores, cabos e sensores), os sistemas digitais (plataformas de dados e automação) e as partes interessadas (município, concessionária e cidadãos).

Uma análise de risco com o objetivo de identificar possíveis ameaças à segurança, à governança e à operação contínua do sistema foi conduzida. Ela permitiu identificar os possíveis pontos de fragilidade que podem comprometer o desempenho e a confiabilidade da infraestrutura crítica, servindo como base para o desenvolvimento de estratégias de ação. O processo incluiu a avaliação da probabilidade de ocorrência de incidentes e o impacto potencial sobre a operação e a população. A análise considerou o contexto regulatório relacionado à segurança cibernética, à governança e à integração entre os diferentes atores envolvidos, como a prefeitura, a concessionária e os consumidores.

Os potenciais problemas críticos de segurança e governança foram identificados na análise de risco, incluindo a vulnerabilidade a ataques cibernéticos direcionados aos dispositivos *IoT* da rede elétrica, a ausência de políticas eficazes de privacidade dos dados dos consumidores e a falta de diretrizes claras sobre a governança dos dados energéticos. Considerando o cenário exposto acima, os frameworks COBIT 2019, ISO/IEC 27001 e NIST Cybersecurity Framework (CSF) apresentam contribuições complementares para o desenvolvimento de um sistema de governança eficaz em *Smart Grids*, especialmente no contexto das cidades inteligentes.

Utilização do COBIT 2019

O COBIT 2019, com sua abordagem centrada na entrega de valor às partes interessadas, permite estruturar a governança de forma alinhada aos objetivos estratégicos da gestão urbana, distribuindo as responsabilidades, definindo controles e oferecendo uma visão completa da infraestrutura de TI. Sua flexibilidade é útil para lidar com as diferentes realidades das cidades inteligentes, que variam em tecnologia, políticas e gestão. Nesse contexto, o COBIT 2019 foi utilizado com base em princípios fundamentais descritos no framework, especialmente no documento *COBIT 2019 Framework: Introduction and Methodology* e no *COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution* [Information Systems Audit and Control Association 2018]. Os princípios aplicados foram:

- **Entrega de valor às partes interessadas:** Ideia central do COBIT 2019, este princípio foca na criação de benefícios mensuráveis para todas as partes envolvidas. No caso da rede elétrica inteligente, isso se traduz na garantia de um fornecimento de energia estável, seguro e eficiente.
- **Abordagem holística:** O COBIT propõe que a governança seja construída a partir de um conjunto integrado de componentes (como processos, estruturas organizacionais, informações, habilidades, cultura e serviços). Essa abordagem foi aplicada para integrar as dimensões de TI, engenharia elétrica, gestão pública e participação da sociedade civil, afim de que nenhuma área crítica seja tratada de forma isolada.
- **Governança de ponta a ponta:** Segundo o COBIT, a governança deve abranger todas as funções, processos e informações relevantes. No contexto da rede elétrica inteligente, isso significa desde os dispositivos físicos, como sensores e medidores inteligentes, até os sistemas avançados de controle baseados em IA.
- **Distinção entre governança e gestão:** O *framework* distingue claramente entre as funções de governança (tomada de decisões, definição de metas e avaliação de desempenho) e as de gestão (planejamento, execução e monitoramento). Essa distinção deve ser aplicada delimitando o papel da prefeitura e da agência reguladora como instâncias de governança, enquanto a concessionária de energia atua como responsável pela gestão operacional dos recursos técnicos.

Aplicação da ISO/IEC 27001

No contexto de cidades inteligentes que operam redes elétricas inteligentes (*Smart Grids*), a aplicação da ISO/IEC 27001 é estratégica para proteger os dados transmitidos e processados por sensores, dispositivos *IoT*, sistemas de medição, plataformas de controle e centros de análise preditiva. Sua adoção permite a implementação de controles baseados em riscos, abrangendo políticas, processos, tecnologias e responsabilidades que garantam a segurança da informação em toda a cadeia de valor dos dados energéticos. A seguir, são apresentadas as principais recomendações de aplicação da norma:

As organizações envolvidas na gestão da rede elétrica inteligente — como concessionárias, prefeituras e órgãos reguladores — implementem um Sistema de Gestão de

Segurança da Informação (SGSI) integrado à governança corporativa. Isso significa que a segurança da informação deve ser tratada como parte essencial da cultura organizacional, sendo incorporada nas decisões estratégicas e operacionais. A definição clara de papéis e responsabilidades, conforme exigido pela norma, ajuda a promover o comprometimento institucional com a proteção da informação em todos os níveis.

Além disso, recomenda-se que as políticas de cibersegurança sejam estabelecidas com base em uma análise de riscos alinhada aos objetivos estratégicos da cidade inteligente, garantindo que a coleta, o armazenamento e o compartilhamento de dados dos consumidores sigam princípios éticos, legais e transparentes. Por fim, a norma requer a implementação de mecanismos de monitoramento, auditoria e melhoria contínua, com base em indicadores mensuráveis. Assim, propõe-se a elaboração de relatórios periódicos, auditorias internas e externas, além de revisões regulares de desempenho do SGSI. Isso assegura transparência, responsabilidade e aprimoramento constante na governança da cibersegurança.

Integração do NIST Cybersecurity Framework

O NIST Cybersecurity Framework, por sua vez, oferece uma estrutura modular e prática para identificar, proteger, detectar, responder e recuperar incidentes de segurança cibernética. Ele é especialmente aplicável ao ecossistema de *Smart Grids* por sua capacidade de lidar com ameaças em tempo real e orientar ações de mitigação baseadas em riscos. A flexibilidade do NIST CSF o torna adequado para ser integrado a sistemas preexistentes de governança, complementando as lacunas deixadas por *frameworks* mais generalistas. O NIST CSF complementa os frameworks COBIT 2019 e ISO/IEC 27001 ao fornecer uma abordagem operacional focada exclusivamente em segurança cibernética — aspecto crítico para redes elétricas inteligentes em cidades altamente digitalizadas.

Tabela 5.4: Pontos Positivos e Negativos dos Frameworks no Contexto *Smart Grid*

	COBIT 2019	**ISO/IEC 27001**	**NIST CSF**
Pontos Positivos	Visão ampla e estratégica; adapta-se a múltiplos contextos	Estrutura robusta para gestão de cibersegurança com foco em riscos e controles	Direto, prático e centrado na proteção de infraestruturas críticas
Pontos Negativos	Exige maturidade organizacional elevada	Implementação pode ser complexa e exigir mudanças culturais e estruturais	Menor foco estratégico ou em governança de valor
Adequação ao Contexto Smart Grid	Alinha TI, energia e governo. Garante valor público	Estabelece um Sistema de Gestão da Segurança da Informação (SGSI) para proteger dados sensíveis da rede	Dá respostas rápidas e claras a riscos cibernéticos

Ao integrar COBIT 2019, ISO/IEC 27001 e NIST CSF, este estudo de caso demonstra como a governança da informação e tecnologia pode ser funcional em diferentes níveis — estratégico, tático e operacional — em ambientes urbanos inteligentes. A relação entre esses arcabouços fortalece, especialmente no contexto das *Smart Grids*, a governança e a tecnologia como pilares das cidades inteligentes, assegurando decisões coerentes, responsabilidades bem definidas e uma gestão alinhada aos princípios de transparência, segurança e sustentabilidade.

5.6. Desafios para a Governança em Cibersegurança em Cidades Inteligentes

Criar um modelo eficiente de governança para a cibersegurança e a proteção de dados em cidades inteligentes constitui uma tarefa multifacetada e desafiadora. Essa complexidade decorre da natureza dinâmica e altamente interconectada desses ambientes urbanos, onde a integração de tecnologias emergentes deve coexistir com requisitos regulatórios, limitações técnicas e fatores socioculturais. Enfrentar esses desafios requer uma abordagem colaborativa, multidisciplinar e adaptável.

Um dos principais entraves técnicos está na diversidade de dispositivos e arquiteturas presentes nas infraestruturas de Internet das Coisas (IoT). A ausência de padrões globais de interoperabilidade compromete a integração eficiente de dispositivos heterogêneos, elevando os riscos associados à vulnerabilidade de sistemas e dificultando a aplicação de políticas de segurança unificadas [Kassab and Darabkh 2020]. Em um cenário no qual sensores, atuadores e sistemas móveis operam de forma distribuída, a gestão segura e eficaz das redes urbanas exige mecanismos de orquestração avançados, que muitas vezes são inexistentes ou subutilizados nas administrações públicas.

Além dos desafios técnicos, as barreiras regulamentares exercem forte influência sobre a adoção de tecnologias promissoras. As leis de proteção de dados, como a LGPD e o GDPR, embora essenciais para garantir a privacidade dos cidadãos, representam entraves à implementação de soluções baseadas em *blockchain* e computação em nuvem, por envolverem requisitos rigorosos de conformidade, localização de dados e responsabilidade compartilhada. Essa tensão entre inovação e conformidade destaca a necessidade de marcos regulatórios que sejam, ao mesmo tempo, robustos e flexíveis, capazes de acompanhar a velocidade das transformações tecnológicas.

Do ponto de vista social, a resistência à mudança e a ausência de cultura de cibersegurança entre gestores públicos, desenvolvedores e usuários finais limitam a efetividade das estratégias de proteção digital [Rani et al. 2021]. A falta de treinamento adequado, somada à percepção de que segurança é um custo adicional e não uma prioridade estratégica, contribui para a adoção fragmentada e reativa de soluções de cibersegurança. Essa lacuna formativa evidencia a importância de políticas de educação digital e capacitação contínua dos profissionais envolvidos na governança urbana.

Outro obstáculo relevante refere-se à fragmentação das regulamentações entre diferentes níveis de governo e jurisdições. Enquanto algumas regiões desenvolvem políticas públicas avançadas de cibersegurança, outras enfrentam dificuldades estruturais para estabelecer normas mínimas de proteção [Meneghello et al. 2019]. Essa disparidade cria um cenário assimétrico e vulnerável, dificultando a implementação de soluções intermunicipais ou interestaduais de segurança. Além disso, a conectividade entre cidades e regiões

torna a segurança de uma área dependente da maturidade da outra, criando riscos sistêmicos para toda a cadeia urbana.

A escassez de financiamento para iniciativas de cibersegurança em projetos de cidades inteligentes constitui um desafio recorrente [Tahirkheli et al. 2021]. Muitos municípios não dispõem de orçamento para incorporar soluções de proteção ou contratar especialistas capacitados. Essa limitação orçamentária compromete a capacidade das cidades de responder adequadamente a incidentes cibernéticos, ampliando a exposição a ataques sofisticados. Em paralelo, a carência de profissionais qualificados agrava o cenário, sendo necessárias estratégias de atração e retenção de talentos em cibersegurança.

Diante desse panorama, torna-se imprescindível adotar estratégias integradas que contemplem aspectos tecnológicos, humanos e institucionais. A combinação entre inovação tecnológica, gestão de riscos baseada em normas internacionais e políticas públicas participativas é o caminho mais promissor para garantir a segurança digital em cidades inteligentes. A promoção de ecossistemas de inovação seguros exige investimentos contínuos em infraestrutura, governança de dados, formação de talentos e marcos regulatórios adaptativos. Por fim, o equilíbrio entre inovação e cibersegurança deve guiar a construção de cidades mais resilientes, sustentáveis e centradas no cidadão. A proteção da privacidade, a integridade das infraestruturas e a confiabilidade dos serviços urbanos são elementos indispensáveis para que a transformação digital se traduza em qualidade de vida, confiança pública e bem-estar social.

5.7. Tendências Futuras e Recomendações

A consolidação das cidades inteligentes representa a emergência de um ecossistema urbano digitalmente interconectado, onde a governança exerce papel estratégico para assegurar a segurança, a confiabilidade e a sustentabilidade das infraestruturas e dos dados gerados em larga escala. Nesse cenário, os profissionais de governança devem estar preparados para lidar com desafios complexos relacionados à cibersegurança, à privacidade da informação e à gestão estratégica de tecnologias disruptivas. Antecipar prioridades emergentes é essencial para orientar políticas públicas, investimentos e a formulação de *frameworks* normativos que apoiem o desenvolvimento seguro desses ambientes urbanos.

Neste contexto, [Ramachandran 2024] propõe cinco prioridades-chave que se mostram altamente relevantes para o futuro da governança digital em cidades inteligentes. A primeira delas é a liderança ativa e persuasiva em cibersegurança, diante do aumento da sofisticação das ameaças impulsionadas por tecnologias emergentes como a inteligência artificial (IA) e a computação quântica. Nesse sentido, recomenda-se a adoção de arquiteturas de segurança robustas, como *DevSecOps* e o modelo *Zero Trust*, que possibilitam uma proteção contínua, proativa e contextualizada das infraestruturas digitais.

A segunda prioridade refere-se à gestão estratégica de tecnologia, reconhecendo que a transformação digital deve caminhar de forma integrada à estratégia organizacional. Em cidades inteligentes, isso implica alinhar tecnologias emergentes a políticas públicas e serviços urbanos, maximizando eficiência, inovação e qualidade de vida. A terceira prioridade destaca a governança de TI como componente essencial da governança urbana, assegurando que os investimentos em tecnologia estejam alinhados a metas institucio-

nais e regulatórias, com foco na gestão de desempenho, riscos e recursos tecnológicos aplicados a serviços críticos como saúde, segurança pública e mobilidade.

A governança de dados, apontada como quarta prioridade, torna-se pilar central em cidades inteligentes devido ao grande volume de dados gerados e utilizados para decisões automatizadas. Garantir qualidade, segurança, privacidade e ética no uso desses dados é imperativo, especialmente frente às legislações de proteção de dados, como a LGPD e o GDPR. Por fim, a gestão de talentos e competências digitais figura como quinta prioridade estratégica. O sucesso da governança digital da cibersegurança depende diretamente da formação contínua de profissionais multidisciplinares e da capacidade de reter talentos em um ambiente de constante inovação e transversalidade tecnológica.

Aplicação de IA e AM na cibersegurança urbana

A complexidade crescente das cidades inteligentes demanda soluções tecnológicas avançadas para proteção de infraestruturas críticas. A Inteligência Artificial (IA) e o Aprendizado de Máquina (AM) têm se destacado como ferramentas promissoras para a detecção proativa de ameaças, análise preditiva de vulnerabilidades e resposta automatizada a incidentes. Como ressaltado por [Merlano 2024], os sistemas baseados em IA são capazes de analisar grandes volumes de dados em tempo real e identificar padrões anômalos que possam indicar comportamentos maliciosos.

Em ambientes urbanos, onde milhares de dispositivos e sensores estão interconectados, a análise de grandes volumes de dados em tempo real é vital para reduzir a superfície de ataque e responder rapidamente a eventos críticos. Além disso, IA e AM permitem a antecipação de riscos cibernéticos, auxiliando gestores na implementação de medidas preventivas mais eficazes. Entretanto, sua eficácia depende da qualidade dos dados utilizados e da integração com outras camadas de defesa. Questões como privacidade, transparência algorítmica e viés devem ser abordadas com rigor, o que reforça a necessidade de diretrizes claras para o uso ético e responsável dessas tecnologias no contexto da governança urbana.

No cenário mundial, o avanço da IA está em ritmo acelerado. Empresas e governos investem bilhões em sistemas que otimizam decisões, automatizam processos e influenciam comportamentos. Mas essa mesma IA pode ser usada para vigilância em massa, manipulação de informações e criação de armas autônomas. Com a ascensão de desafios geopolíticos e a necessidade de uma governança mais inclusiva e sustentável, as políticas globais ajudam a definir padrões éticos, técnicos e jurídicos para o uso seguro da tecnologia. Elas também promovem a troca de informações entre países e estabelecem mecanismos de resposta a incidentes. Sem esse tipo de coordenação, cada país age por conta própria, o que favorece lacunas e brechas exploradas por atores mal-intencionados.

Aqui é importante enfatizar iniciativas como a PartNIR (Parceria BRICS para a Nova Revolução Industrial) que busca não apenas a diversificação tecnológica, mas também a criação de ecossistemas soberanos de IA. A PartNIR é uma iniciativa estratégica dos países do BRICS (Brasil, Rússia, Índia, China e África do Sul) destinada a promover a diversificação e atualização tecnológica da base industrial desses países. Essa iniciativa visa ao desenvolvimento e à integração das cadeias produtivas dos membros do grupo, focando especialmente na inovação e na adoção de novas tecnologias. Ela também visa

fortalecer a segurança cibernética através do desenvolvimento de tecnologias que sejam adaptadas às realidades e aos idiomas dos países do grupo, garantindo assim uma competitividade sustentável no cenário global.

Os objetivos principais da PartNIR são o adensamento e integração das cadeias produtivas, o desenvolvimento de ecossistemas soberanos de inteligência artificial e a atualização tecnológica da base industrial. Embora a PartNIR não seja específica para o contexto de cidades inteligentes, ela terá grandes impactos nas mesmas haja visto que busca promover a cooperação industrial entre os países do BRICS e a modernização das indústrias, visando à criação de cadeias de valor mais robustas e interconectadas que possam competir eficazmente no mercado global. A IA é vista como uma revolução no conhecimento e na tecnologia, com um grande potencial. Contudo, para que esses benefícios sejam compartilhados, é necessária uma governança global justa e equitativa. O BRICS, sob liderança brasileira, propõe uma estrutura que promova o desenvolvimento sustentável e inclusivo, defendendo o acesso não-discriminatório à transferência de tecnologia, protegendo dados pessoais e garantindo a integridade das informações para um uso ético e responsável da IA.

Uso de *Blockchain* para autenticação e proteção de dados

A tecnologia *blockchain* também desponta como uma aliada estratégica para fortalecer a autenticação e a proteção de dados nas cidades inteligentes. Sua estrutura descentralizada e imutável oferece resistência a ataques e falhas centralizadas, aumentando a confiança em transações digitais e no gerenciamento de identidades. Conforme discutido por [Bhushan et al. 2020], a tecnologia *blockchain* pode ser integrada às infraestruturas urbanas para permitir autenticação segura de cidadãos, dispositivos e serviços.

A tecnologia também favorece a gestão de permissões de acesso e a rastreabilidade de interações com dados sensíveis. Contudo, sua adoção em larga escala exige atenção a desafios técnicos, como o consumo energético e a escalabilidade. É fundamental estabelecer padrões técnicos e normativos que guiem sua implementação de forma interoperável e compatível com legislações de proteção de dados.

Implementação do modelo *Zero Trust* em infraestruturas urbanas

O modelo de segurança *Zero Trust*, baseado na premissa de que nenhuma entidade deve ser automaticamente confiável, tem se consolidado como abordagem eficaz contra ameaças sofisticadas em ambientes urbanos. Ele exige autenticação contínua, políticas de acesso dinâmicas e segmentação de rede, reduzindo significativamente o risco de movimentos laterais de atacantes e acessos não autorizados. A aplicação do *Zero Trust* em cidades inteligentes requer rever o projeto das arquiteturas tradicionais, incorporando controle contextual de acesso e análise comportamental. Essa abordagem permite aos gestores maior visibilidade e controle sobre os fluxos de dados e acessos em tempo real. No entanto, sua efetividade depende da constante atualização das políticas de segurança e da integração com outras camadas de defesa cibernética, conforme ressaltado em [Kaur et al. 2023].

Essas tendências apontam para uma governança de cibersegurança mais resiliente, dinâmica e centrada no cidadão. A integração de tecnologias emergentes, combinada à

capacitação de talentos e à formulação de políticas inclusivas e éticas, será essencial para enfrentar os desafios complexos da era das cidades inteligentes.

5.8. Considerações Finais

A crescente digitalização dos ambientes urbanos, impulsionada pelo avanço das cidades inteligentes, demanda um olhar atento à governança da cibersegurança e da privacidade dos dados. Esse processo exige não apenas a adoção de tecnologias inovadoras, como *IoT* e dispositivos móveis, mas também o fortalecimento de políticas públicas, estruturas regulatórias e boas práticas organizacionais voltadas à cibersegurança. A proteção de infraestruturas críticas e dados sensíveis depende da capacidade de governos e organizações implementarem modelos de governança robustos, adaptáveis e integrados à realidade urbana. Este capítulo apresentou uma abordagem teórica para compreender os fundamentos da governança da cibersegurança, discutir os principais frameworks normativos — como NIST CSF, ISO/IEC 27001 e COBIT 2019 — e identificar os desafios e práticas associadas à gestão de dispositivos conectados em cidades inteligentes. A análise do estudo de caso demonstrou que, embora cada arcabouço tenha suas limitações, sua combinação estratégica atende a diferentes níveis de maturidade tecnológica, possibilitando desde respostas operacionais até o alinhamento estratégico com metas institucionais.

A revisão sistemática da literatura evidenciou lacunas importantes na padronização e na interoperabilidade de dispositivos, na descentralização da tomada de decisão e na ausência de diretrizes específicas para contextos urbanos. Além disso, foram destacados desafios técnicos e regulatórios, especialmente quando se trata da aplicação de *frameworks* em cidades com limitações de infraestrutura, capacitação técnica e recursos financeiros. Tais fatores reforçam a necessidade de um olhar mais adaptativo, contextualizado e multidisciplinar para a construção de soluções eficazes de governança de cibersegurança. As tendências emergentes, como a aplicação de inteligência artificial, *blockchain* e modelos de confiança zero, oferecem caminhos promissores para o fortalecimento da segurança cibernética em ecossistemas urbanos complexos. No entanto, sua efetividade está condicionada à existência de estratégias de governança claras, baseadas em princípios éticos, democráticos e transparentes. O futuro da cibersegurança nas cidades inteligentes depende da capacidade de articulação entre tecnologia, política, sociedade e ciência, com investimentos contínuos em pesquisa, capacitação e inovação.

Por fim, espera-se que os conhecimentos discutidos ao longo do capítulo sirvam como base para que pesquisadores, estudantes e profissionais desenvolvam ações práticas e políticas mais eficazes na área de cibersegurança urbana. A governança da cibersegurança, longe de ser uma tarefa exclusivamente técnica, deve ser pensada como um projeto coletivo, voltado à proteção dos direitos digitais dos cidadãos e à construção de cidades mais resilientes, seguras e inclusivas. O fortalecimento dessa agenda é essencial para garantir que o avanço tecnológico caminhe lado a lado com o respeito à privacidade, à equidade e à sustentabilidade urbana.

Agradecimentos

Este trabalho foi realizado com o apoio do Programa de Excelência Acadêmica da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - PROEX CAPES. Os au-

tores agradecem o apoio da UTFPR, UFPR e da UFMG e o auxílio financeiro da FAPESP #2018/23098-0 e 2024/09341-0 e do CNPq #444824/2024-3, #440553/2024-5 e #313844/2020-8.

Referências

[Ahmadi-Assalemi et al. 2020] Ahmadi-Assalemi, G., Al-Khateeb, H., Epiphaniou, G., and Maple, C. (2020). Cyber resilience and incident response in smart cities: A systematic literature review. *Smart Cities*, 3(3):894–927.

[Bhushan et al. 2020] Bhushan, B., Khamparia, A., Sagayam, K. M., Sharma, S. K., Ahad, M. A., and Debnath, N. C. (2020). Blockchain for smart cities: A review of architectures, integration trends and future research directions. *Sustainable Cities and Society*, 61:102360.

[Brezolin et al. 2024] Brezolin, U., Nakayama, F., and Nogueira, M. (2024). Detecçao de varreduras de portas pela análise inteligente de tráfego de rede IoT. In *Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais (SBSeg)*, pages 271–286. SBC.

[Brito et al. 2023] Brito, D., de Neira, A. B., Borges, L. F., and Nogueira, M. (2023). An autonomous system for predicting DDoS attacks on local area networks and the Internet. In *2023 IEEE LATINCOM*, pages 1–6, Panama. IEEE.

[Buckwald and Marchant 2021] Buckwald, J. M. and Marchant, G. E. (2021). Improving soft law governance of the internet of things. *IEEE Technology and Society Magazine*, 40(4):101–114.

[Camargo et al. 2024] Camargo, E. T., Martins, L. D., and Fonseca, K. V. O. (2024). *Smart sensors for smart environment*, chapter Chapter 5, pages 67–89.

[Camargo et al. 2021] Camargo, E. T., Spanhol, F. A., and Castro e Souza, A. R. (2021). Deployment of a lorawan network and evaluation of tracking devices in the context of smart cities. *Journal of Information Security and Applications*, 12(8):1–24.

[de Neira et al. 2020] de Neira, A. B., Araujo, A. M., and Nogueira, M. (2020). Early botnet detection for the Internet and the Internet of Things by autonomous machine learning. In *Proceedings of the 16th International Conference on Mobile Ad Hoc and Sensor Networks (MSN)*, pages 516–523, Japan.

[Demidov et al. 2018] Demidov, R., Zegzhda, P. D., and Kalinin, M. O. (2018). Threat analysis of cyber security in wireless adhoc networks using hybrid neural network model. *Automatic Control and Computer Sciences*, 52:971–976.

[Elmaghraby and Losavio 2014] Elmaghraby, A. S. and Losavio, M. M. (2014). Cyber security challenges in smart cities: Safety, security and privacy. *Journal of Advanced Research*, 5(4):491–497.

[Frandell and Feeney 2022] Frandell, A. and Feeney, M. (2022). Cybersecurity threats in local government: A sociotechnical perspective. *The American Review of Public Administration*, 52(8):558–572.

[Goumopoulos 2024] Goumopoulos, C. (2024). Smart city middleware: A survey and a conceptual framework. *IEEE Access*, 12:4015–4047.

[Gracias et al. 2023] Gracias, J. S., Parnell, G. S., Specking, E., Pohl, E. A., and Buchanan, R. (2023). Smart cities—a structured literature review. *Smart Cities*, 6(4):1719–1743.

[Ham 2021] Ham, J. V. D. (2021). Toward a better understanding of "cybersecurity". *Digital Threats: Research and Practice*, 2(3):1–3.

[Hatcher et al. 2020] Hatcher, W., Meares, W. L., and Heslen, J. (2020). The cybersecurity of municipalities in the united states: An exploratory survey of policies and practices. *Journal of Cyber Policy*, 5(2):302–325.

[Hossain et al. 2024] Hossain, S. T., Yigitcanlar, T., Nguyen, K., and Xu, Y. (2024). Understanding local government cybersecurity policy: A concept map and framework. *Information*, 15(6):342.

[Information Systems Audit and Control Association 2018] Information Systems Audit and Control Association (2018). *COBIT® 2019 Framework: Governance and Management Objectives*. ISACA.

[Kassab and Darabkh 2020] Kassab, W. and Darabkh, K. A. (2020). A–z survey of internet of things: Architectures, protocols, applications, recent advances, future directions and recommendations. *Journal of Network and Computer Applications*, 163:102663.

[Kassakian et al. 2011] Kassakian, J., Schmalensee, R., Desgroseilliers, G., Heidel, T., Afridi, K., Farid, A., Grochow, J., Hogan, W., Jacoby, H., Kirtley, J., Michaels, H., Perez-Arriaga, I., Perreault, D., Rose, N., and Wilson, G. (2011). The future of the electric grid: An interdisciplinary mit study.

[Kaur et al. 2023] Kaur, R., Gabrijelčič, D., and Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion*, 97:101804.

[Laprie et al. 2004] Laprie, J.-C., Randell, B., and Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 1(1):11–33.

[Lee et al. 2021] Lee, E., Seo, Y.-D., Oh, S.-R., and Kim, Y.-G. (2021). A survey on standards for interoperability and security in the internet of things. *IEEE Communications Surveys & Tutorials*, 23(2):1020–1047.

[Lipner and Anderson 2018] Lipner, S. and Anderson, R. (2018). CIA history. *Personal commun.*

[Melaku 2023] Melaku, H. M. (2023). A dynamic and adaptive cybersecurity governance framework. *Journal of Cybersecurity and Privacy*, 3(3):327–350.

[Meneghello et al. 2019] Meneghello, F., Calore, M., Zucchetto, D., Polese, M., and Zanella, A. (2019). Iot: Internet of threats? a survey of practical security vulnerabilities in real iot devices. *IEEE Internet of Things Journal*, 6(5):8182–8201.

[Merlano 2024] Merlano, C. (2024). Enhancing cyber security through artificial intelligence and machine learning: A literature review. *Journal of Cyber Security*, 6.

[Nogueira 2022] Nogueira, M. (2022). Governança e regulamentações do mercado de sistemas em nuvem. Technical Report RT.DCC.003/2022, Universidade Federal de Minas Gerais e Huawei Brasil.

[Nogueira et al. 2024] Nogueira, M., Borges, L. F., de Neira, A. B., Albano, L., and Coelho, K. K. (2024). Ciência de dados aplicada à cibersegurança: Teoria e prática. *Minicursos do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 1–50.

[Nogueira et al. 2021] Nogueira, M., Borges, L. F., and Nakayama, F. (2021). Das redes vestíveis aos sistemas ciber-humanos: Uma perspectiva na comunicação e privacidade dos dados. *SBRC, Sociedade Brasileira de Computação*.

[Ometov et al. 2019] Ometov, A., Bezzateev, S., Voloshina, N., Masek, P., and Komarov, M. (2019). Environmental monitoring with distributed mesh networks: An overview and practical implementation perspective for urban scenario. *Sensors*, 19(24):5548.

[Pardini et al. 2017] Pardini, D. J., Heinisch, A. M. C., and Parreiras, F. S. (2017). Cyber security governance and management for smart grids in brazilian energy utilities. *JISTEM-Journal of Information Systems and Technology Management*, 14:385–400.

[Pascoe 2023] Pascoe, C. E. (2023). Public draft: The nist cybersecurity framework 2.0. *National Institute of Standards and Technology*.

[Pastório et al. 2023] Pastório, J. a., Castro e Souza, A. R., Spanhol, F., Huff, A., and De Camargo, E. T. (2023). Alr-lorawan: An application-level retransmission management algorithm for lorawan networks. Latin-American Symposium on Dependable and Secure Computing (LADC) '23, page 11–20, New York, NY, USA. ACM.

[Pastório et al. 2020] Pastório, A., Rodrigues, L., and de Camargo, E. (2020). Uma revisão sistemática da literatura sobre tolerância a falhas em internet das coisas. In *Anais Estendidos do X Simpósio Brasileiro de Engenharia de Sistemas Computacionais*, pages 57–64, Porto Alegre, RS, Brasil. SBC.

[Pavlenko and Zegzhda 2018] Pavlenko, E. and Zegzhda, D. (2018). Sustainability of cyber-physical systems in the context of targeted destructive influences. In *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*, pages 830–834. IEEE.

[Ramachandran 2024] Ramachandran, R. (2024). Five key priorities for governance practitioners in 2025. Accessed: 2025-04-06.

[Rani et al. 2021] Rani, S., Mishra, R. K., Usman, M., Kataria, A., Kumar, P., Bhambri, P., and Mishra, A. K. (2021). Amalgamation of advanced technologies for sustainable development of smart city environment: A review. *IEEE Access*, 9:150060–150087.

[Rao and Deebak 2023] Rao, P. M. and Deebak, B. D. (2023). Security and privacy issues in smart cities/industries: technologies, applications, and challenges. *Journal of Ambient Intelligence and Humanized Computing*, 14(8):10517–10553.

[Ribeiro et al. 2023] Ribeiro, A. V., Nakayama, F., and Nogueira, M. (2023). Um panorama dos serviços de saúde avançados: Conectividade e segurança em sistemas de vida assistida. *Minicursos do Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos*, pages 1–50.

[Sarker et al. 2021] Sarker, I. H., Furhad, M. H., and Nowrozy, R. (2021). Ai-driven cybersecurity: an overview, security intelligence modeling and research directions. *SN Computer Science*, 2(3):173.

[Sedrati et al. 2022] Sedrati, A., Ouaddah, A., Mezrioui, A., and Bellaj, B. (2022). Iotgov: an iot governance framework using the blockchain. *Computing*, 104(10):2307–2345.

[Serrano et al. 2022] Serrano, M., Griffor, E., Wollman, D., Dunaway, M., Burns, M., Rhee, S., and Greer, C. (2022). Smart cities and communities: A key performance indicators framework. *NIST Special Publication*, 1900:206.

[Siddiqui et al. 2024] Siddiqui, S., Hameed, S., Shah, S. A., Arshad, J., Ahmed, Y., and Draheim, D. (2024). A smart-contract-based adaptive security governance architecture for smart city service interoperations. *Sustainable Cities and Society*, 113:105717.

[Slongo et al. 2024] Slongo, J., Lindino, C., Martins, L. D., Spanhol, F. A., Carneiro, E., and Camargo, E. T. (2024). Evaluation of low-cost sensors to integrate in a water quality monitor for real-time measurements. *Environmental Monitoring and Assessment*, 196(8):716.

[Tahirkheli et al. 2021] Tahirkheli, A. I., Shiraz, M., Hayat, B., Idrees, M., Sajid, A., Ullah, R., Ayub, N., and Kim, K.-I. (2021). A survey on modern cloud computing security over smart city networks: Threats, vulnerabilities, consequences, countermeasures, and challenges. *Electronics*, 10(15):1811.

[Takkouche and Norman 2011] Takkouche, B. and Norman, G. (2011). Prisma statement. *Epidemiology*, 22(1):128.

[Webb and Hume 2018] Webb, J. and Hume, D. (2018). Campus iot collaboration and governance using the nist cybersecurity framework. In *Living in the Internet of Things: Cybersecurity of the IoT-2018*, pages 1–7. IET.

[Wilkins and Mifsud 2024] Wilkins, A. W. and Mifsud, D. (2024). What is governance? projects, objects and analytics in education. *Journal of Education Policy*, 39(3):349–365.

[Xagoraris et al. 2023] Xagoraris, L., Kogias, D., and Karkazis, P. (2023). A review of zero trust security framework (ztf) for sustainable and resilient smart cities. In *Proceedings of the 27th Pan-Hellenic Conference on Progress in Computing and Informatics*, pages 269–273.

[Yuliana and Hasibuan 2022] Yuliana, R. and Hasibuan, Z. A. (2022). Best practice framework for information technology security governance in indonesian government. *International Journal of Electrical and Computer Engineering*, 12(6):6522.

[Yusif and Hafeez-Baig 2021] Yusif, S. and Hafeez-Baig, A. (2021). A conceptual model for cybersecurity governance. *Journal of applied security research*, 16(4):490–513.

